+ EN CADEAU : 2 magazines complets offerts SUR LE CD

LES CAHIERS DU HACKER

PIRATE [INFORMATIQUE]

PIRATE [INFORMATIQUE] // 38

LE GUIDE DU PIRATE

60 HACKS & CRACKS

100% HACKING
AVEC CD GRATUIT
> TOP Logiciels & Services

Mots de passe

Fossil

Surveillance

Clé USB

Résistance

Media Center

Smartphone

Films & Séries

0% PUB 0 CENSURE

PHISHING

COMMENT ÇA MARCHE ?
UNE ÉTUDE DE CAS
POUR TOUT SAVOIR

ANONYMAT

VIBER, TELEGRAM,
SIGNAL, WHATSAPP :
QUI CACHE QUOI ?

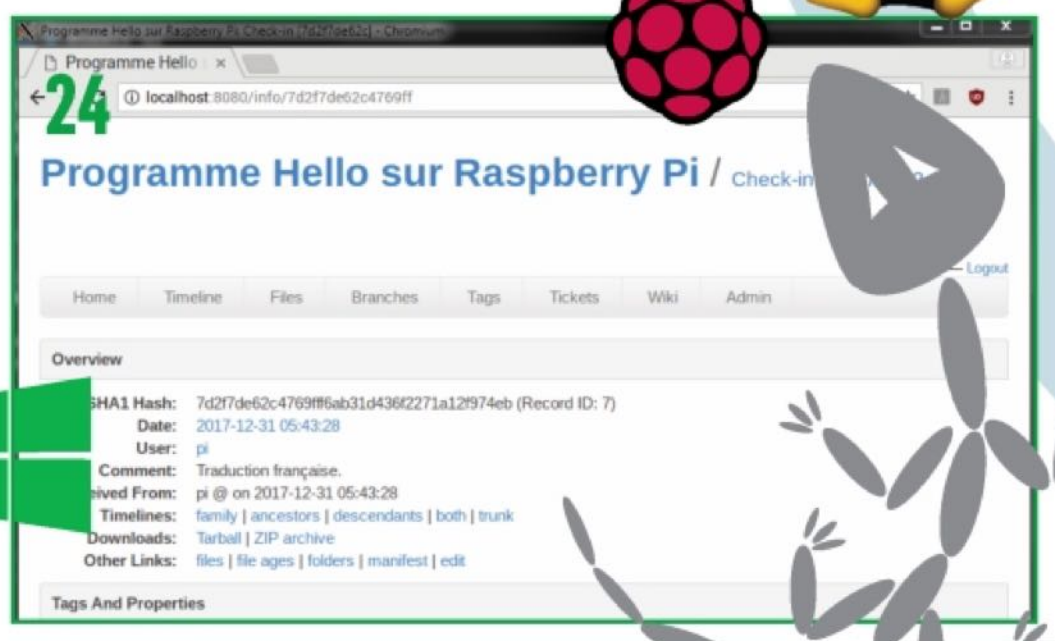
TESTING

PIRATER LA
MACHINE À CAFÉ
PAR CLONAGE NFC !

SOMMAIRE

PROTECTION/ANONYMAT

HACKING



SOUTENEZ-NOUS !

Vous découvrez ce magazine en l'ayant téléchargé illégalement ? C'est de bonne guerre, nous sommes pour le partage ! Merci de l'intérêt que vous portez à nos articles, mais pour que nous puissions continuer l'aventure, pensez à acheter le magazine : offrez-le, parlez-en autour de vous ! *Pirate Informatique* existe depuis presque 9 ans, sans publicité et sans hausse de prix depuis 7 ans.

CONCERNANT NOTRE CD

Certains lecteurs inquiets nous envoient régulièrement des e-mails concernant notre CD. Ce dernier serait selon eux rempli de virus en tout genre ! Il s'agit bien sûr de faux positifs. Les détections heuristiques des antivirus ne s'appuient pas sur les signatures de malwares, mais sur les comportements des logiciels. Et il faut bien reconnaître que certains des logiciels que nous plaçons sur le CD ont des comportements semblables à des programmes malveillants. Bref, il n'y a pas de virus sur nos galettes. Ce serait dégoûtant non ?

LES CAHIERS DU HACKER
PIRATE [INFORMATIQUE]

N°38 - Août - Octobre 2018

Une publication du groupe ID Presse.
27, bd Charles Moretti - 13014 Marseille
E-mail : redaction@idpresse.com

Directeur de la publication :
David Côme

McNulty : Benoît Bailleul

Major Crimes Unit : Esteban Mauvais, Marc Delb, la team Bl@ckBird, The Lone Gunman et Thibaut Le Corre du Parti Pirate

Kima & Bunk : Sergueï Afanasiuk & Stéphanie Compain

Correctrice : Marie-Line Bailleul

Imprimé en France par / Printed in France by :
Léonce Deprez
ZI Le Moulin 62620 Ruitz

Distribution : MLP

Dépôt légal : à parution

Commission paritaire : en cours

ISSN : 1969 - 8631

«Pirate Informatique» est édité par SARL ID Presse, RCS : Marseille 491 497 665
Parution : 4 numéros par an.

ÉDITO

BONJOUR AUX HABITUÉS COMME AUX NOUVEAUX VENUS !

Vous avez peut-être remarqué que la mode était au chiffrement, en ligne ou localement. On voit parfois des clés USB «cryptées» vendues 3 fois leur prix alors qu'avec un logiciel français comme VeraCrypt, il est possible de faire la même chose sur une clé normale ! Nous vous expliquerons comment faire et nous verrons aussi les autres fonctionnalités de ce programme. Esteban nous propose cette fois d'en apprendre plus sur les autorisations/permissions d'Android et nous en saurons plus sur le phishing avec la team Bl@ckBird. Notre ami The Lone Gunman nous expliquera quant à lui les subtilités du clonage de puces NFC. Pour ce n°38 nous continuons d'offrir un peu d'espace d'expression à nos camarades du Parti Pirate avec cette fois un sujet d'actualité : la réforme du droit d'auteur au niveau européen.

N'oubliez pas de vous abonner à la mailing-list ou à nous suivre sur Twitter pour vous tenir au courant des actus et nous rapprocher de vous en attendant le prochain numéro (voir page 49).

N'hésitez pas à nous faire part de vos commentaires et de vos souhaits pour les prochaines éditions sur **benbailleul@idpresse.com**

Bonne lecture !

Benoît BAILLEUL.

HACKTUALITÉS

IL Y A VRAIMENT DU MONDE POUR DÉFENDRE GOOGLE ?

Google va sans doute écoper d'une amende record par la Commission européenne pour «abus de position dominante». Elle reproche en fit à la société américaine de forcer les constructeurs de smartphones à préinstaller sa suite logicielle. Alors que nous pensions que notre position vis-à-vis de cette amende était majoritaire, nous avons pourtant vu ça et là sur Internet que ce n'était pas le cas : il y a vraiment des gens qui pensent que Google est «victime» d'une pseudo kabbale antiaméricaine. Premièrement, la Commission européenne sanctionne Google car il empêche l'émergence de plusieurs acteurs dans son secteur. Dominer son secteur n'est pas puni par la loi, mais empêcher des concurrents de grandir oui. Quand vous avez un concurrent en face, curieusement vous êtes bien plus innovant : demandez à Intel, dépassée par AMD au début des années 2000 et qui est revenu à force de travail et de R&D. Reviens aussi souvent la rengaine : « *Mais personne n'est obligé d'utiliser Google* ». Effectivement, mais c'est oublier que tout le monde n'a pas la même aisance avec l'informatique et aujourd'hui beaucoup de personnes pensent que leur page d'accueil Google c'est «Internet», sans parler des moteurs de recherche par défaut intégrés à certains navigateurs ou OS. C'est justement ce qui est décrié par la Commission : certains fabricants auraient certains avantages à mettre Chrome en navigateur par défaut. Pourquoi ne pas laisser le choix ? Google devenu une entreprise au pouvoir démesuré. Nous n'avons rien contre cette compagnie qui popularise aussi l'open source, mais ce pouvoir vient de cet abus de position dominante et aussi d'optimisation fiscale qui lui fait payer très peu d'impôt. Les startups en face de Google ne peuvent prétendre à de tels montages. La solution pour elle : se vendre (à Google !) ou mourir. Cette sanction de 2,4 milliards, avec potentiellement 6 milliards en plus, n'est qu'un caillou dans la chaussure de Google... Il est aussi amusant de noter que le *moto* de Google était «*Don't be Evil*» depuis le début de l'aventure, mais il a récemment disparu des documentations internes.

Yannick Favennec Becot est un homme politique encarté à l'UDI. Lorsqu'on lui a ressorti des Tweets de 2009, il ne les a pas tout de suite reconnus comme les siens. Premier réflexe : ***« Mon compte Tweetter a été hacker !! »*** (sic). Ha ben non en fait.

Un faille qui rend Dingo

Un hacker fan de Mickey a réussi à pirater le système Fastpass de Disneyland Paris. Rappelons que cette technologie permet de passer plus vite aux attractions très populaires en régulant le flux des visiteurs (vous avez un créneau horaire pour vous présenter et couper la queue). Le pirate Artex a réussi à contourner ce système en modifiant le QR Code imprimé sur les fameux tickets Fastpass. Il s'était rendu compte que les numéros de ces tickets étaient consécutifs et a simplement fait du reverse engineering pour obtenir des codes valides sur son smartphone. Au lieu de vendre sa trouvaille, il a prévenu le parc qui l'a remercié. Très fair play de sa part d'autant que les Fastpass générés utilisaient les places «réservées» par d'autres visiteurs au même créneau.

UN TEL DEGRÉ DE CONNERIE, C'EST DE L'ART

«I Agree» c'est à la fois le bouton sur lequel vous vous empressez d'appuyer ou de cliquer lorsque vous installez une appli, un programme ou quand vous souscrivez à un service, mais c'est aussi une œuvre d'art ! Pour illustrer la longueur des CGU (conditions générales d'utilisation) de certaines applis, le designer Dima Yarovinsky a «déroulé» le contenu pour montrer le côté absurde de cette demande. Sur des papiers de couleurs différentes, l'artiste a entrepris d'imprimer les textes rédigés par Facebook, Instagram, Snapchat ou Twitter. Notons que non seulement personne ne lit ces textes imbuvables, mais pour une raison bien simple : il faudrait par exemple plus d'une heure pour les 12 000 mots de la CGU de Snapchat.

RAMPAGE, UNE FAILLE CRITIQUE ? EN THÉORIE SEULEMENT...

Après HeroRAT et les malwares véhiculés par de fausses applis du jeu Fortnite, c'est un mois chargé pour les possesseurs de smartphones Android puisque des chercheurs néerlandais ont dernièrement découvert une faille de sécurité qui pourrait potentiellement frapper tous les appareils sortis depuis 2012. Baptisée RAMPage, cette faille utilise la technique dite de «martèlement» (rowhammer) qui consiste à modifier les données stockées dans la RAM. Pour outrepasser les permissions et restrictions de l'OS, il s'agit de modifier des cellules mémoires qui se trouvent «à côté» des cellules auxquelles l'appli malveillante à accès. Ceci permet donc à une application d'accéder à des secteurs qu'elle ne devrait pas être autorisée à lire. Tout cela est bien sûr théorique, car même si l'exploitation de cette faille a pu être réalisée en laboratoire, il faudrait une dose incroyable de chance pour récupérer des informations sensibles par exemple. Google a d'ailleurs annoncé qu'aucun patch n'est prévu pour boucher cette faille tout en remerciant les chercheurs pour leur travail. C'est ce qui s'appelle être sûr de son coup...

HACKTUALITÉS

TÉLÉCHARGER, C'EST VOLER ?

On nous le rabâche sans arrêt : télécharger c'est voler ! Le problème c'est que c'est complètement faux. Il suffit de réfléchir quelques minutes pour comprendre que ce discours bien huilé ne sert qu'à culpabiliser les uns et à marginaliser les autres. Quelles sont les couleuvres qu'on veut nous faire avaler ?

Lorsqu'on écoute les têtes bien pensantes de l'industrie du cinéma, du jeu vidéo et de la musique, c'est évident et ça ne souffre d'aucune contestation : le piratage c'est du vol ! Le lavage de cerveau a commencé il y a longtemps déjà et on ne se souvient même plus qui a commencé avec ce *running gag*. Si vous allez à la FNAC et que vous volez «physiquement» un CD, ce dernier se retrouve dans votre poche et plus dans les rayons : c'est du vol. Dans le cas des téléchargements, cet album est juste copié. S'il est à votre goût, peut-être l'achèterez-vous... Bien sûr c'est illégal, mais la quantité croissante de biens culturels disponibles oblige à faire un choix, car notre budget «CD/DVD» reste le même... pour les plus chanceux.

UN ALBUM TÉLÉCHARGÉ =UNE VENTE PERDUE?

Pour enfoncer le clou, les majors ont toujours propagé l'idée qu'un fichier téléchargé c'est une vente en moins. Mais achèteriez-vous tous les films ou MP3 que vous téléchargez ? Bien sûr que non. L'amalgame entre téléchargement et vol sert à faire paraître le crime plus grave qu'il ne l'est. Le P2P a même tendance à encourager les ventes ! Combien d'artistes connaissent une véritable notoriété grâce à Internet ? Le bouche-à-oreille comme le fait que la musique soit disponible immédiatement de chez soi propagent à grande vitesse la notoriété des gens talentueux (Laurie étant l'exception qui confirme la règle).

UN ARTISTE ÇA VEND DES CD. POINT.

Comme elles n'ont pas vraiment la côte auprès des P2Pistes, les majors ont alors joué sur la corde sensible en déclarant que les agissements des «pirates» revenaient à prendre directement l'argent des artistes. Pour que cela soit vrai, il faudrait que les artistes soient réduits à de simples vendeurs de CD. Or ce n'est pas le cas ! Un chanteur ou un groupe de musique gagne de l'argent sur les recettes des concerts et sur les produits dérivés bien plus qu'avec la vente de ses CD. Et même si cela était vrai, il faut s'appeler David Guetta ou Joey Starr ou pour gagner suffisamment avec les royalties. Dans tous les cas, ce sont les majors qui ramassent le pactole. Télécharger un album ce n'est donc pas comme si vous braquiez Dalida, Bézu ou les Hansons. C'est juste ce qu'on essaie de vous faire croire...

L'AMALGAME ENTRE TÉLÉCHARGEMENT ET VOL SERT À FAIRE PARAÎTRE LE CRIME PLUS GRAVE QU'IL NE L'EST.

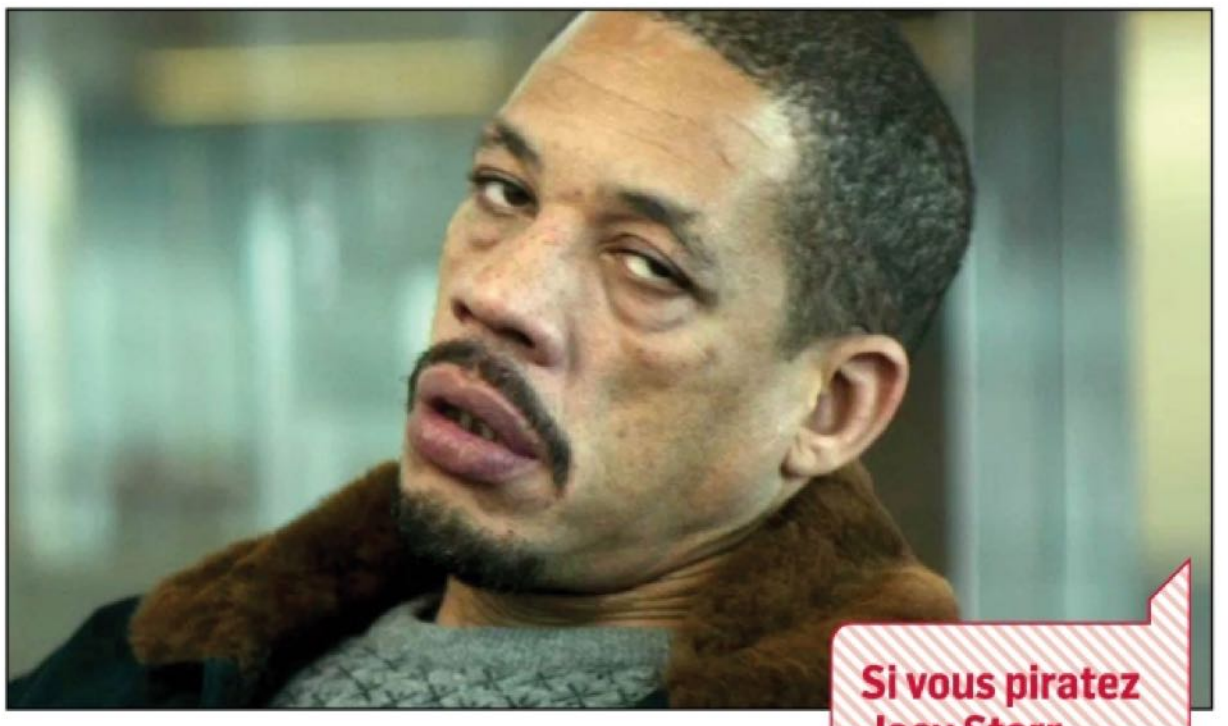
La vérité est ailleurs

Au Japon, le «piratage» est très marginal, car les producteurs proposent souvent des «petits plus» avec leur CD ou leur DVD : CD bonus, cadeau, goodies, etc. Le produit devient un «objet» que l'on collectionne et le prix est accepté par les consommateurs. En France, rares sont les artistes qui proposent autre chose que le «boîtier crystal» standard. Et en dématérialisé c'est encore pire puisqu'on a... RIEN. Les majors vous expliqueront que les marges sont déjà trop courtes pour ajouter une peluche, un porte-clé ou même un booklet avec les paroles.

HOCKTUALITÉS

LE TÉLÉCHARGEMENT EST RESPONSABLE DE LA CHUTE DES VENTES?

Un autre mensonge est aussi servi à toutes les sauces : si les ventes de CD/DVD chutent, c'est à cause du téléchargement. Il faut d'abord préciser que les supports physiques sont en concurrence avec des tas d'autres formats, et même avec d'autres formes de divertissement : jeux vidéo, VOD, Internet, etc. On a moins de temps à consacrer à la musique, on achète donc moins de musique, en CD ou en dématérialisé. Pire, le disque compact est complètement dépassé ! À l'heure des smartphones de plusieurs Gigaoctets, une galette comporte toujours entre 12 et 20 pistes. Et après, on s'étonne que les CD de ses poulains se vendent mal... Ce phénomène n'est pas nouveau, les industries du disque et du cinéma ont toujours montré du doigt les améliorations technologiques, car elles annonçaient pour elles la fin de leurs années de gloire. Tour à tour, la télévision, le magnétoscope, la K7 audio ont été dans le viseur des majors. Elles ont pourtant su s'adapter et Universal existe toujours ! Le P2P, le MP3 et les DivX seraient-ils si puissants qu'ils détruiraient tout sur leur passage ?



Si vous piratez Joey Starr, il viendra se venger à la machette ! Allez donc le voir en concert...

LA CONTREFAÇON, LE VRAI PROBLÈME!

C'est un phénomène de plus en plus vivace et dont personne ne parle : la véritable contrefaçon, celle que l'on voit sur les marchés ou sous les manteaux et qui n'a rien à voir avec le monde du P2P... Car pour les majors, «le méchant pirate» c'est celui qui télécharge l'intégrale des Beatles avec BitTorrent alors que les albums sont rentabilisés depuis des années. Personne ne parle du véritable pirate qui télécharge l'intégrale de tout ce qui bouge pour vendre à la sauvette du contenu copié comme on peut en voir dans certains pays asiatiques ou de l'Est.

LES DOSSIERS DU

Pirate

DES DOSSIERS THÉMATIQUES COMPLETS

- PETIT FORMAT
- MINI PRIX
- CONCENTRÉ D'ASTUCES

À DÉCOUVRIR EN KIOSQUES

100% Windows

Actuellement #Guide pratique

BEST-OF LOGICIELS GRATUITS

Le nouveau site
des utilisateurs
ANDROID

- ✓ Des dizaines de tutoriels et dossiers pratiques
- ✓ Mobiles & Tablettes : des tests complets !
- ✓ Sélection des meilleures applis + des vidéos et du fun !

Android MT
Solutions & Astuces

www.android-mt.com

IL REVIENT !

CRÉER UN VIRUS SUR ANDROID, C'EST FACILE !

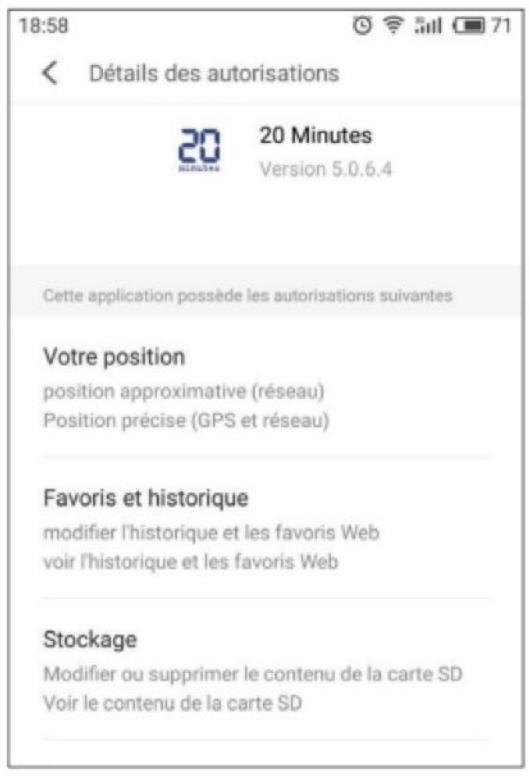
(MAIS C'EST MAL)

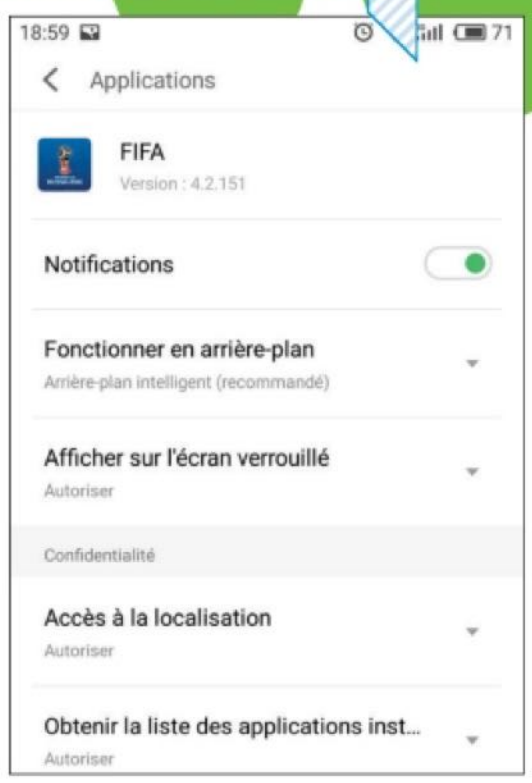
Comme vous pouvez le constater, tous les jours des programmes vous demandent des autorisations. Que ce soit sur votre ordinateur, votre smartphone ou même vos appareils Bluetooth, tous sans exception demandent votre permission. À force de les voir partout, on ne les lit même plus, on clique sur Accepter et on va parfois jusqu'à grogner à cause de la redondance !

Merci à Esteban Mauvais de la Monkey Co. pour cet article !
https://themonkey.co

Au fil du temps, on a pu constater que pas mal de failles ont permis d'outrepasser les demandes de permissions, et ce, sur la plupart des systèmes d'exploitation actuels ! Ce ne serait même pas étonnant d'en découvrir d'autres, les programmes sont devenus tellement complexes qu'il est difficile de faire un logiciel parfait. Afin de comprendre un peu mieux pourquoi les permissions sont essentielles et pas juste une pop-up relou, on va prendre l'actualité comme exemple : Aujourd'hui, nous ne pouvons pas forcer un utilisateur au stockage de

Sur un portable Android récent, il est possible de voir facilement les autorisations accordées à chaque application. Si vous avez accepté trop vite, il n'est pas trop tard pour aller jeter un œil..





LEXIQUE

***PERMISSION/AUTORISATION :** Android est issu d'un noyau Linux. Il reprend en particulier son modèle de sécurité basé sur un système de permissions. Une application a un accès exclusif à ses propres fichiers et aucune autre application n'est capable de venir fouiller dans ses affaires. Sauf si vous lui donnez la permission. Lorsque vous installez une application, celle-ci vous demande d'avoir accès à vos contacts, vos appels, votre appareil photo, etc. C'est parfois justifié, mais parfois non. Si vous refusez la permission, l'appli risque de ne pas s'installer... à moins de lui forcer la main sur un mobile rooté.

cookies sur son navigateur Web et donc on ne peut pas faire de statistiques valables sans son accord. Avant, un simple message de prévention suffisait à indiquer la récolte de statistiques.
Les permissions sont une protection de votre vie privée, du contrôle de votre machine et surtout un moyen simple de demander votre consentement !

MESSENGER DEMANDE PLUS D'UN TIERS DE TOUTES LES PERMISSIONS

Maintenant qu'on vient de voir toute l'importance des permissions sur vos machines, parlons d'une rumeur. En 2014, l'application Facebook Messenger est victime d'une rumeur, celle de vous espionner !
Pourquoi donc ? Car au moment de l'installation, l'application vous demande une grande panoplie d'autorisations sur votre localisation, votre identité, votre micro, votre caméra et j'en passe ! Cette rumeur est légitime, mais fausse. En effet, il suffit de vérifier ce qui tourne en tâche de fond, ce qui est envoyé aux serveurs de Facebook ou même d'aller décortiquer le code source de l'application ! Ceci étant dit, cette rumeur est allée tellement loin que le 22 mai 2018 Mark

PAS À PAS

Comment fonctionnent les permissions ?

01 ACCÈS AU MICRO

Tout d'abord, pour demander la permission d'accéder au micro du téléphone, il suffit de mettre cette ligne :
<uses-permission android:name=»android.permission.RECORD_AUDIO» />
Il suffit ensuite de créer une classe avec les bonnes librairies :
package com.android.audiorecordtest;

import android.Manifest;
import android.content.Context;

```
<manifest xmlns:android="http://schemas.android.com/apk/res/androi
    package="com.callrecorder"
    android:versionCode="1"
    android:versionName="1.0">

    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.SYSTEM_ALERT

    <uses-permission android:name="android.permission.RECORD_AUDIO
    <uses-permission android:name="android.permission.PROCESS_OUTG
    <uses-permission android:name="android.permission.READ_PHONE_S
    <uses-permission android:name="android.permission.WAKE_LOCK" />

    <uses-sdk
        android:minSdkVersion="16"
        android:targetSdkVersion="22" />

    <application
      android:name=".MainApplication"
```

import android.content.pm.PackageManager;
import android.media.MediaRecorder;
import android.os.Bundle;
import android.support.v4.app.ActivityCompat;
import android.support.v7.app.AppCompatActivity;

import java.io.IOException;

public class MonVirus extends AppCompatActivity {
}

02 ENREGISTRER CE QUE LE MICRO CAPTE

On pourrait tout simplement créer ensuite une fonction qui contient l'enregistrement puis la sauvegarde dans un fichier :
mRecorder = new MediaRecorder();
mRecorder.setAudioSource(MediaRecorder.AudioSource.MIC);
mRecorder.setOutputFormat(MediaRecorder.OutputFormat.THREE_GPP);
mRecorder.setOutputFile(mFileName);

Zuckerberg a démenti que Messenger espionne les utilisateurs en tâche de fond ! Entre nous, aucun membre de ce parlement n'était apte à poser les bonnes questions au fondateur de Facebook. Le débat était terriblement ridicule, ils auraient pu faire l'effort de demander de l'aide à la CNIL ou à un autre organisme. Quelques bons arguments sont sortis de cette audition, mais en règle général, beaucoup de flan. Passons aux fourneaux et donnons vie à cette rumeur en fabriquant une appli maline... Attention, nous éviterons bien sûr de détailler les étapes sinon l'article risque de faire 12 pages !

mRecorder.setAudioEncoder(MediaRecorder.AudioEncoder.AMR_NB);
Et pour faire tout ceci en tâche de fond, rien de plus simple :
<service android:name=».MonVirus» android:exported=»false»/>

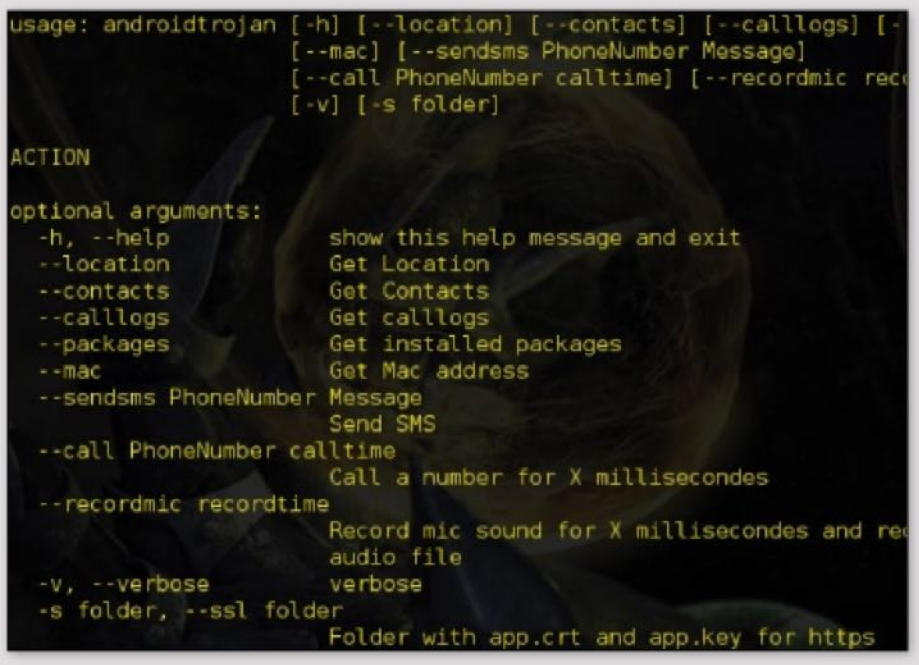
03 UN CAS D'ÉCOLE : SPY CAMERA OS

Derrière tout ça, on peut faire une boucle pour enregistrer des fichiers d'une certaine longueur, les envoyer sur un serveur puis les détruire ! Pour aller encore plus loin, on pourrait ensuite lire tout ceci en direct via une page Web et un peu

d'Ajax ! Le micro c'est bien, mais la caméra c'est mieux, pour cela je vous invite à directement récupérer le code source de Spy Camera OS, en effet cette application d'espionnage est totalement open source et disponible un peu partout sur le Net. Vous écoutez et vous voyez, pourquoi pas, mais c'est un peu nul, ce n'est pas rentable et la principale intention des hackers c'est avant tout de de faire un billet sur votre ignorance ! Comment faire un maximum d'argent assez facilement alors ?

04 TROJANDROID

Ceci est mon ultime réponse, Trojandroid est comme son nom l'indique un trojan destiné à Android et celui-ci est totalement open source et disponible sur Github. Le programme de serveur pour les contrôles est aussi disponible sur le même projet ! OK donc c'est un trojan mais il fait quoi ce truc ? Eh bien plein de choses, il peut envoyer des SMS à votre place, faire des appels, récupérer la liste des programmes installés, récupérer vos contacts, récupérer votre localisation, vous envoyer des publicités et du phishing via notification (d'où la récupération de la liste de vos applis, il peut par exemple se faire passer pour Facebook) et cette application est très facile à camoufler en Tetris par exemple... Encore plus simple, avec **trojandroid_mixapk**, vous pouvez transformer n'importe



quelle appli Android normale en véritable trojan ! Maintenant j'espère que vous ferez attention aux permissions des applications...

MOBILE / DESKTOP

4 MESSAGERIES CHIFFRÉES DANS LE VENT

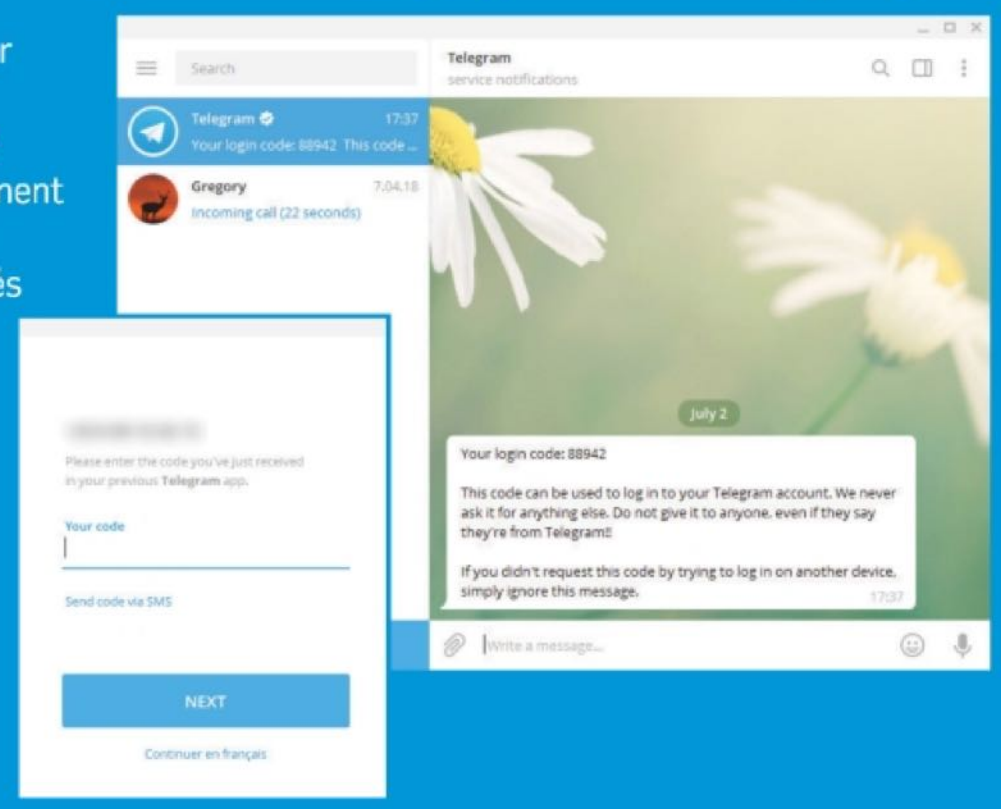
De plus en plus les Internautes prennent conscience de l'importance du respect de la vie privée sur Internet. Devant la demande croissante de solution chiffrée, les éditeurs de logiciels se mettent au diapason. Non seulement des solutions nouvelles se développent, mais les «vieux lions» ajoutent une couche de chiffrement alors que leurs solutions n'en comportaient pas auparavant... Voici notre petite sélection non exhaustive.

LEXIQUE

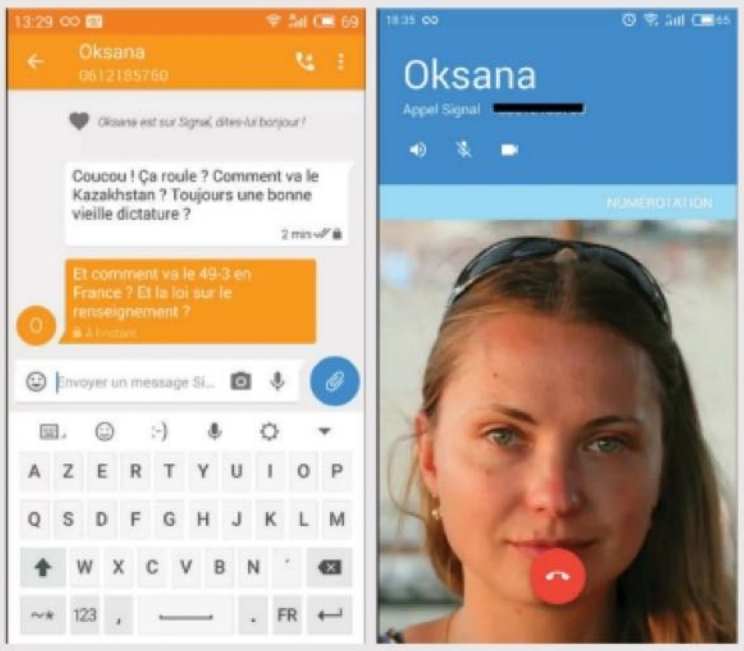
***CHIFFREMENT DE BOUT EN BOUT :**
Ou «end-to-end» dans la langue de Kim Kardashian (l'anglais pas le hobbit, suivez un peu !). Il s'agit d'un système de communication où seules les personnes impliquées peuvent lire les messages échangés. Il évite le problème d'écoute électronique, car les clés ne sont pas échangées sur le réseau.

TELEGRAM

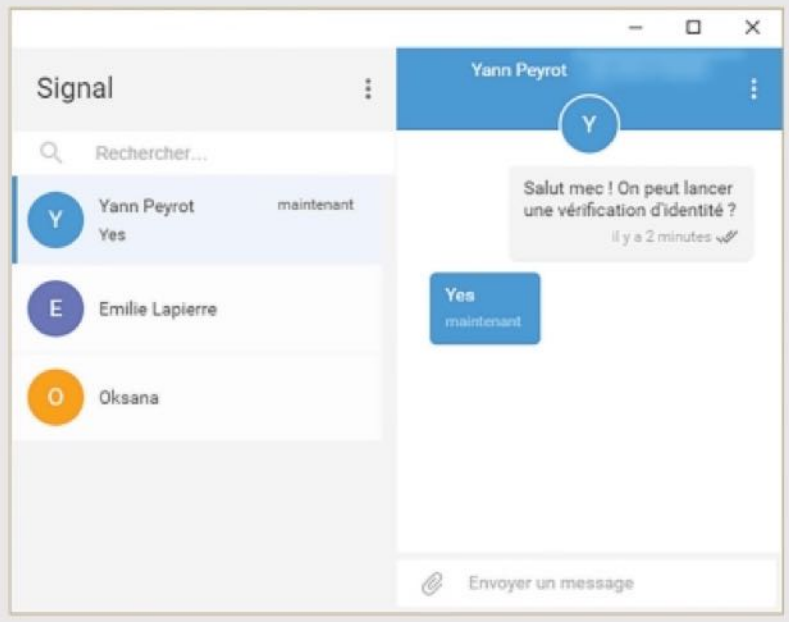
Pointée du doigt pour avoir le malheur d'être utilisée par des djihadistes, Telegram est une application de chat pour mobile et ordinateur. Complètement chiffrés de bout en bout en AES 256 bits, les messages ne sont pas stockés sur un serveur, ils ne font que transiter. La création d'un compte se fait à la manière de Whatsapp avec une vérification par numéro de téléphone. Si vos contacts téléphoniques disposent de Telegram vous serez alors aussitôt au courant. Notez qu'il est aussi possible de s'envoyer des pièces jointes chiffrées jusqu'à un poids de 1,5 Go et qu'il est possible de créer



SIGNAL PRIVATE MESSENGER

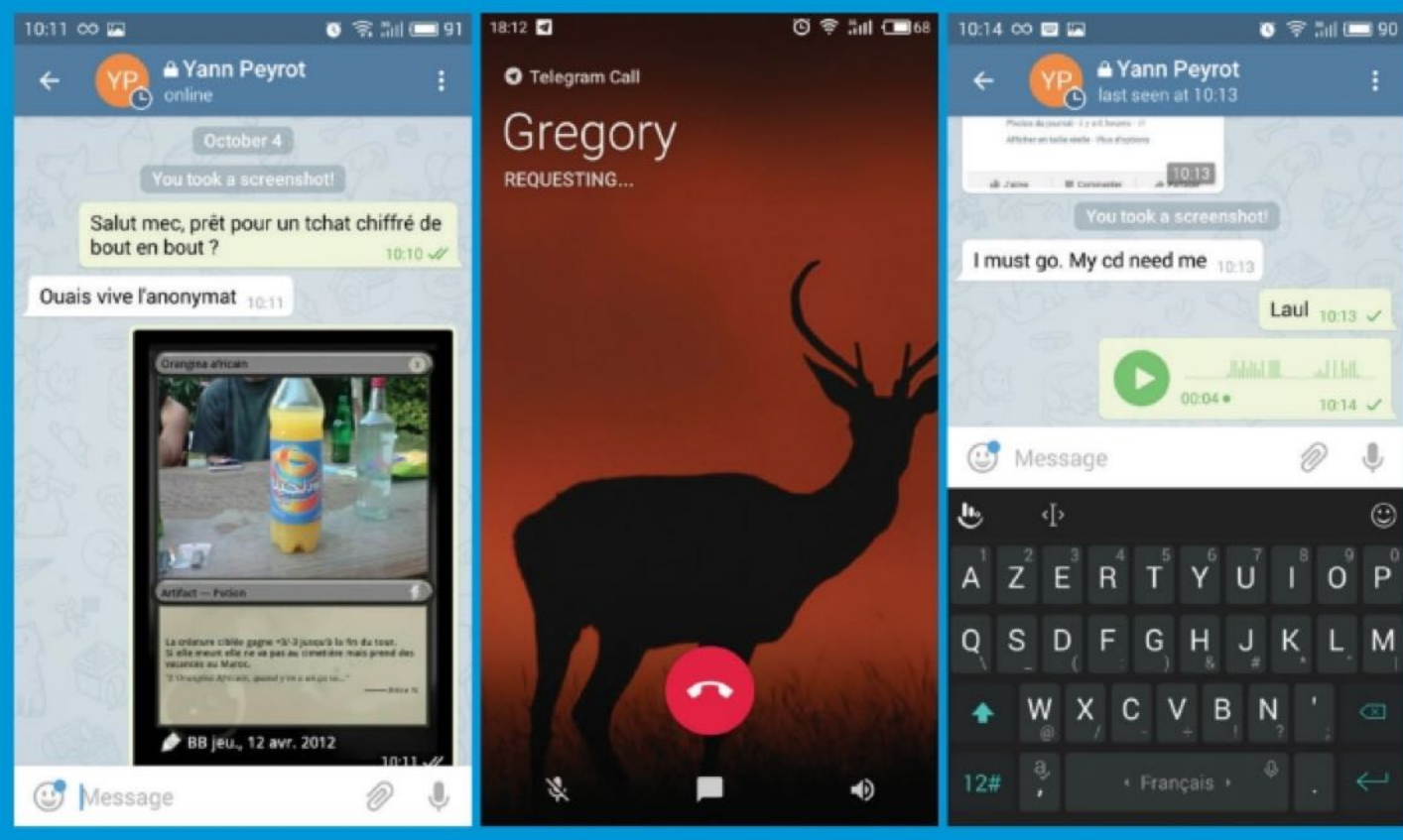


Signal est une appli adoubée par l'ami Snowden lui-même. Gratuite, sans pub et open source, difficile de faire mieux que cette dernière. Signal propose pourtant d'activer la conversation téléphonique à la manière de WhatsApp. On note aussi la possibilité d'importer les SMS pour envoyer des textos depuis la même interface, mais attention, ces derniers ne seront pas chiffrés. Et c'est justement ce qui nous intéresse ici, puisque Signal propose un chiffrement de bout en bout. Pour ce type de protection, impossible pour l'utilisateur de commencer une conversation sur un appareil (mobile) pour la finir sur un autre (ordinateur) et vice-versa. Une solution à base d'extension Chrome a été trouvée (avec une association du téléphone), mais il existe des versions pour desktop qui proposent la même chose depuis novembre 2017. Sur Signal il est aussi possible de passer des appels téléphoniques et des chats en visio. Moins en vue que Telegram c'est pourtant une très bonne alternative qui propose une méthode de couplage mobile/desktop via QR code.



Lien : **https://whispersystems.org**

des canaux et des messages groupés. La version Web fait aussi très bien le travail. Pour cette dernière ou les versions sur PC, il faudra coupler votre compte mobile (si vous en avez un) avec un code envoyé sur votre téléphone. Les appels téléphoniques sont disponibles depuis l'année dernière. Notez que Telegram est libre pour la partie client, mais pas pour la partie serveur. Ce serait problématique si les messages chiffrés n'étaient pas exclusivement chiffrés de bout en bout...

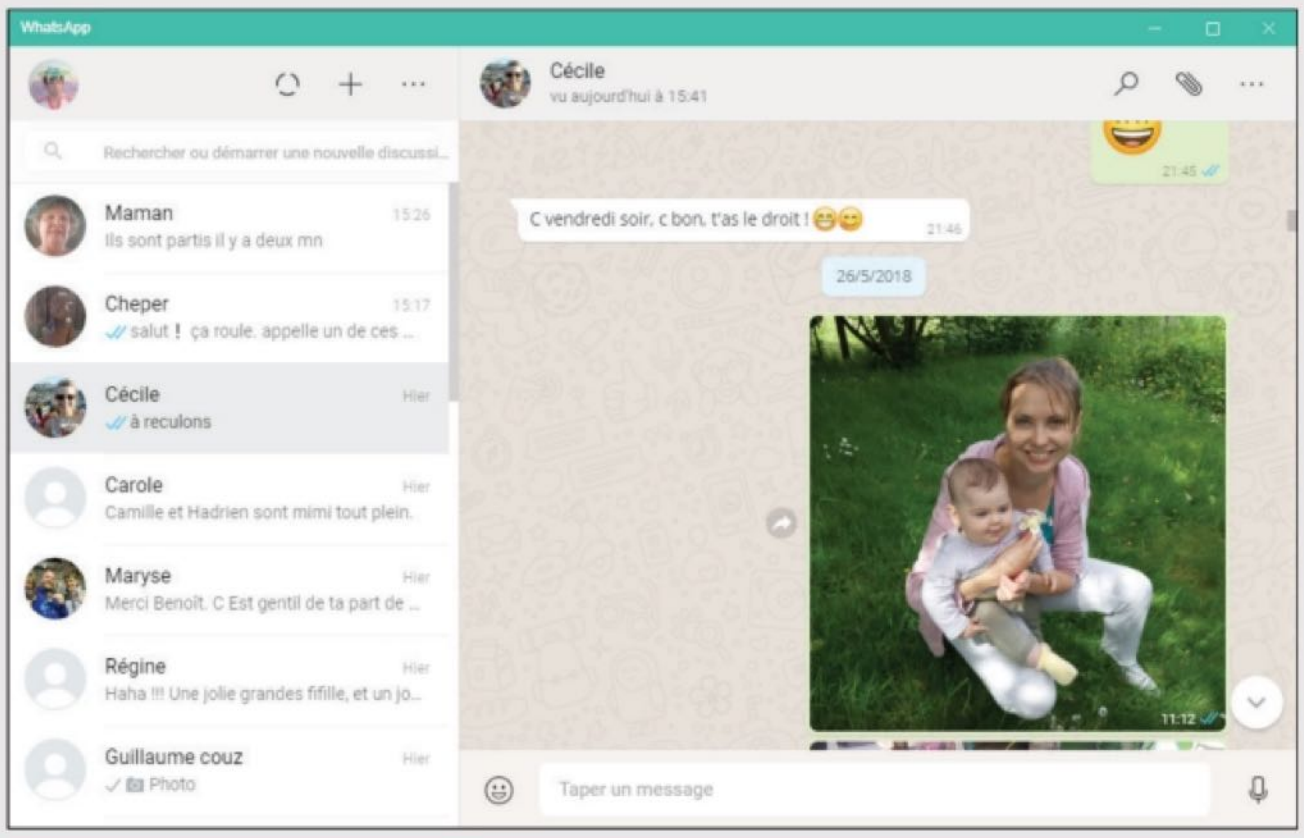


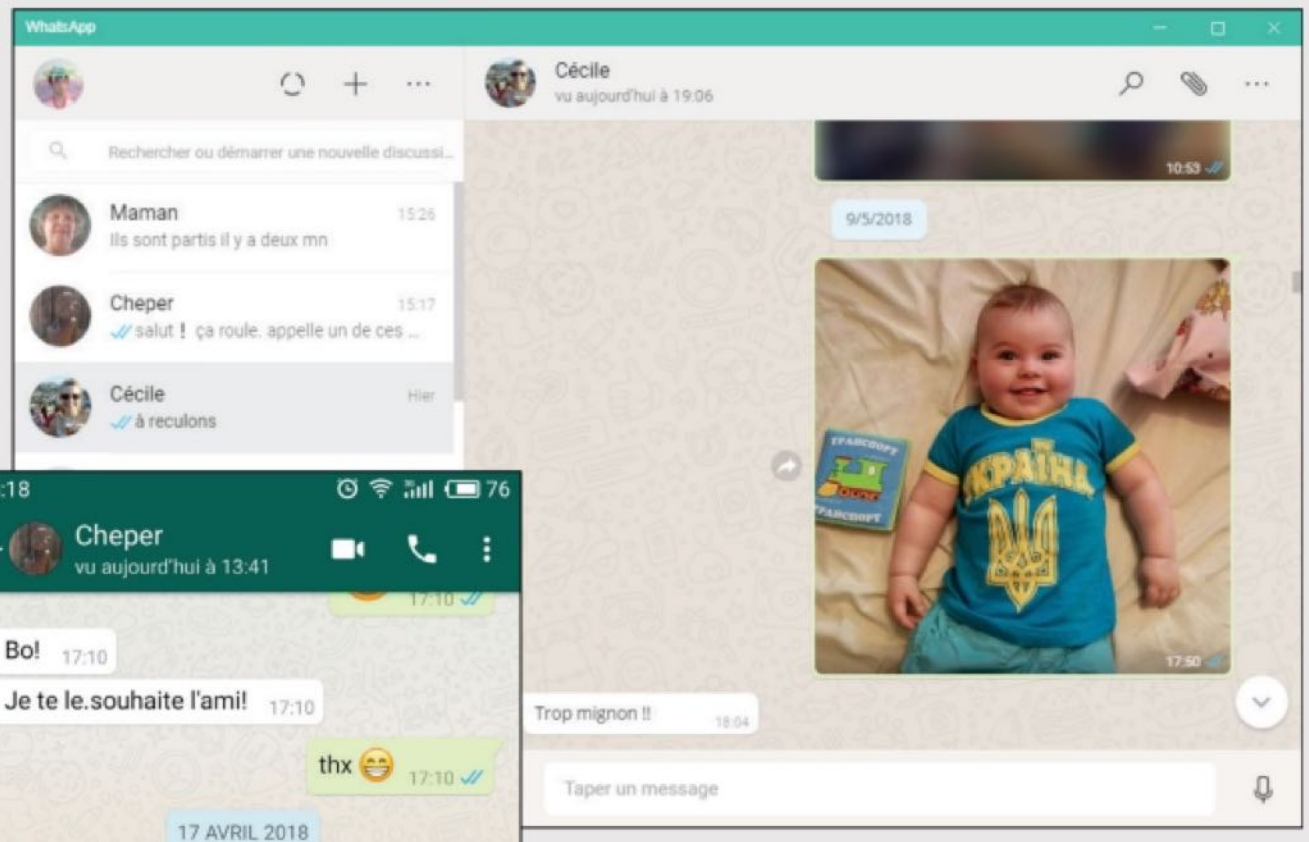
Lien : **https://telegram.org**

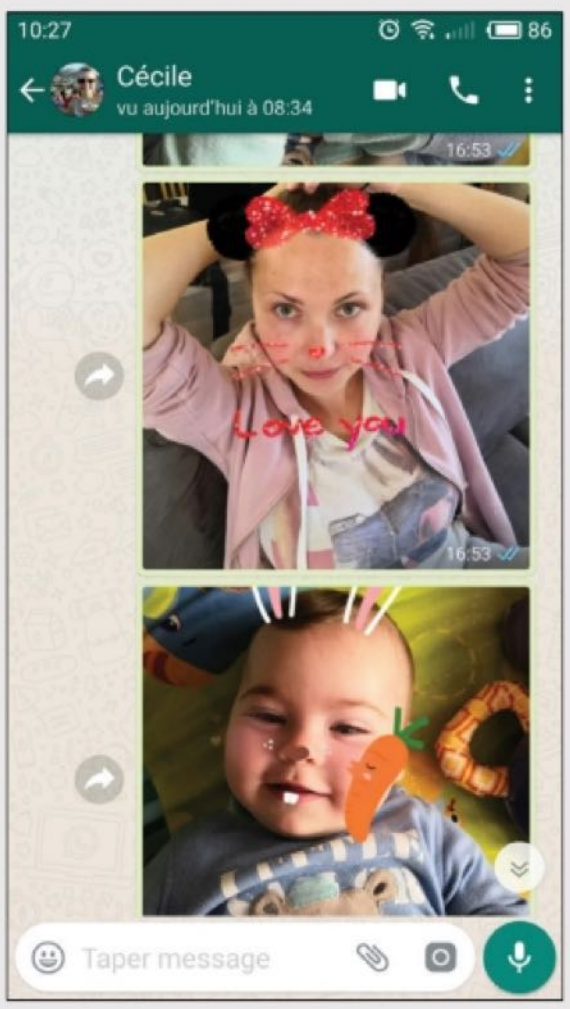
WHATSAPP

WhatsApp est utilisée par un milliard d'utilisateurs et elle est de loin la solution de messagerie n°1. En ajoutant une couche de chiffrement, l'appli a suivi le mouvement de nombreuses messageries. Par la suite, Facebook a flairé la bonne affaire en achetant l'application pour 19 milliards de dollars. Seulement, voilà, le réseau social tentaculaire souhaite utiliser WhatsApp pour faire de la publicité ciblée en se servant de l'énorme base de données que constituent les numéros de téléphone des utilisateurs. Donc oui, avec WhatsApp vos communications sont chiffrées, mais en utilisant votre numéro de téléphone (qui fait office d'identifiant sur cette appli), Facebook peut quand même vous «pister». Cela ne veut pas dire que la société peut lire vos messages : elle se contentera de mieux cibler les publicités qu'elle vous propose par Facebook. Si vous n'avez pas Facebook, pas de problème ! Mais nous pouvons comprendre que le principe vous chagrine. Reste que WhatsApp est de loin l'appli la plus utilisée, nous ne pouvions pas ne pas en parler d'autant que la VoIP est de la partie et qu'elle est de très bonne qualité. Comme pour Signal, le rapprochement entre la partie mobile et la partie sur ordinateur se fait via QR code.

Lien : **www.whatsapp.com**



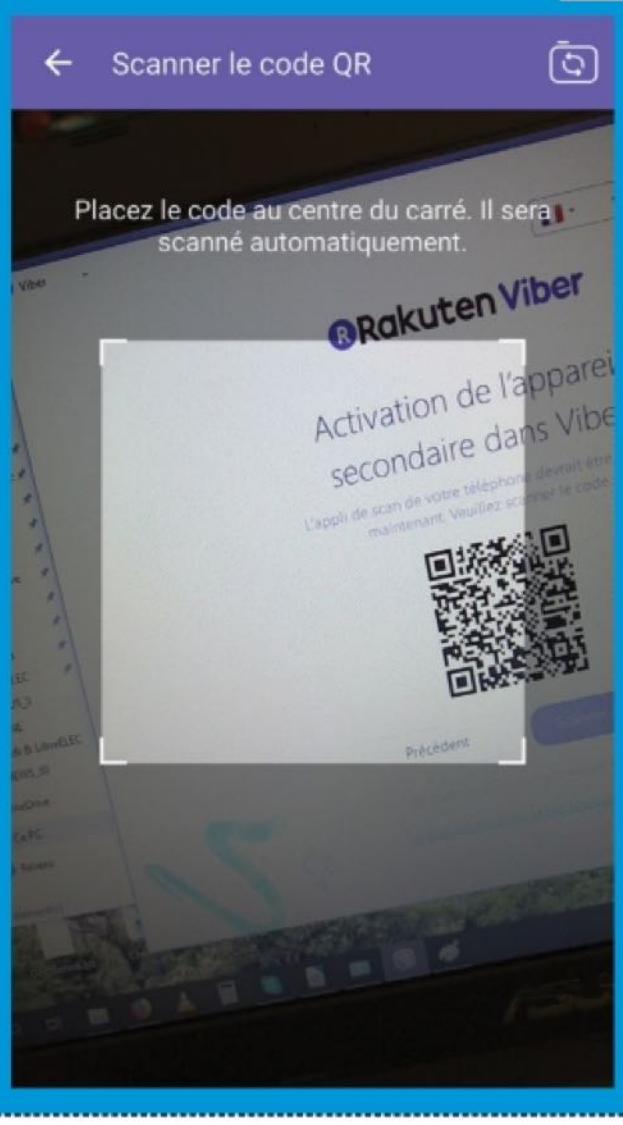


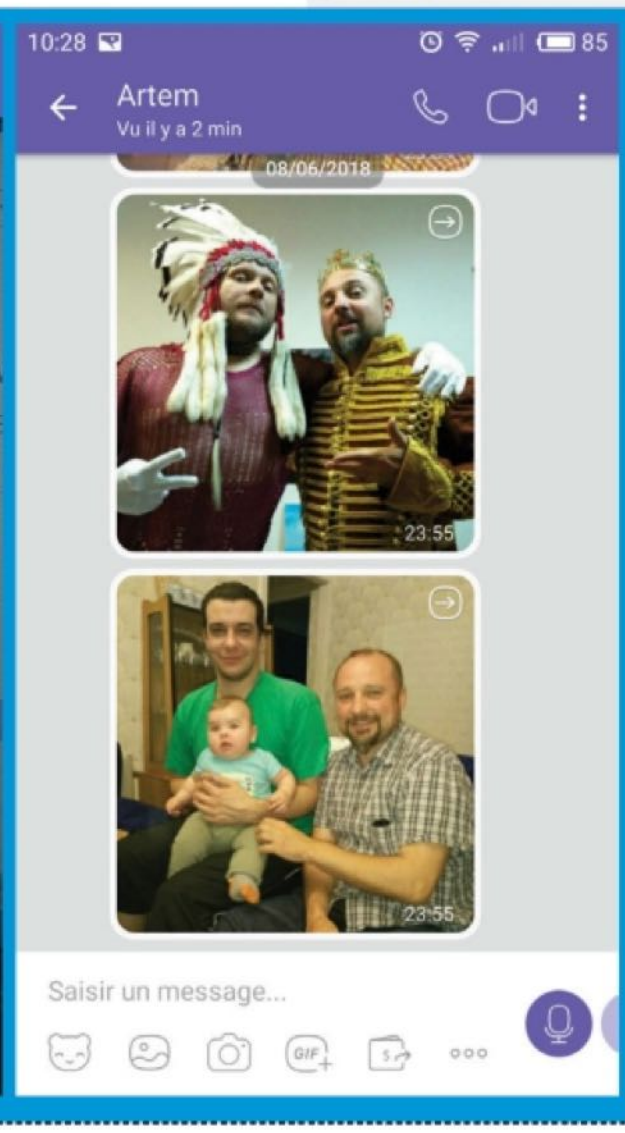


RAKUTEN VIBER

Viber est aussi une messagerie très prisée qui se rapproche plus de Skype avec la possibilité d'appeler sur des téléphones fixes avec l'option Viber Out (canal non chiffré). Pour le reste, Viber a aussi implémenté le chiffrement de bout en bout pour les communications dans lesquelles tous les participants utilisent la dernière version de l'application. Pour rajeunir son image, Viber s'est aussi dotée d'une fonctionnalité de messagerie éphémère comme chez Snapchat. Il est aussi possible d'envoyer de l'argent via un partenariat avec Western Union. L'option chat de groupe est aussi possible tout comme la possibilité de synchroniser la version mobile et la version desktop avec un QR code.

Lien : **www.viber.com/fr**



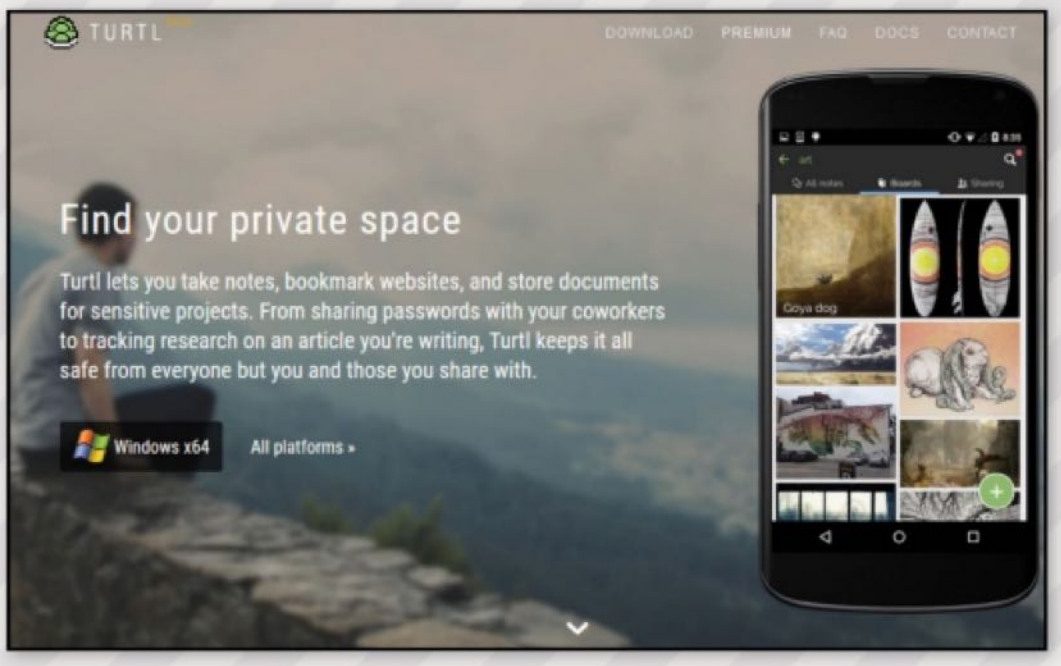


#1 Prenez vos notes en toute sécurité

AVEC TURTL

Microsoft OneNote ou Google Keep pour ne citer que les plus connus, de nombreux services et applications permettent de prendre des notes, stockées dans le Cloud. Ce qui pose évidemment un problème de sécurité. La particularité de Turtl, c'est que vos données sont chiffrées, donc illisibles tant pour d'éventuels pirates que pour les propriétaires du service lui-même. Notez que le programme est multi-plate-forme (Windows, Android, Linux, OSX et bientôt iOS). Turtl autorise le partage de notes avec vos collaborateurs. Il vous faut activer la fonction lors de la création de votre compte. Après avoir renseigné les informations usuelles, il faudra entrer de nouveau l'adresse mail utilisée et un alias (le nom que verront les gens avec qui vous partagerez des notes). Validez avec **Enable sharing**.

Lien : **https://turtlapp.com**



#2 Des tests d'Antivirus

AVEC AV-TEST

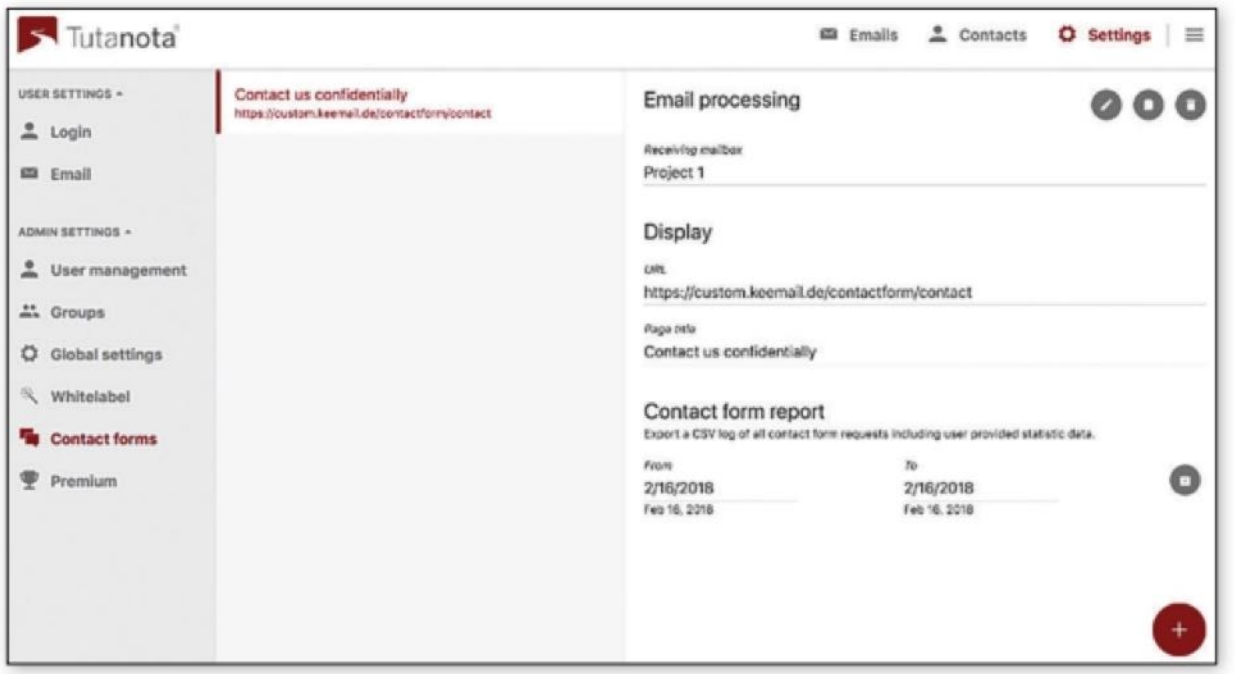
AV-Test est l'institut de recherche indépendant allemand pour la sécurité informatique. Depuis plus de 15 ans, les spécialistes de Magdeburg procèdent à des tests de qualité comparatifs et individuels sur tous les produits de sécurité informatique de niveau international. L'une des plus grandes banques de logiciels malveillants au monde, le centre de recherches de l'institut ainsi que l'intense coopération avec d'autres institutions garantissent des tests reconnus à l'échelle internationale. Pour cela, AV-Test utilise des systèmes d'analyse développés dans ses propres laboratoires, garantissant ainsi des résultats qui ne sont pas influencés par des tiers et qui sont toujours compréhensibles pour tous les systèmes d'exploitation et les plates-formes courants. De plus, AV-Test effectue des recherches sur la sécurité de produits IoT et e-santé, d'applications pour les appareils mobiles ainsi que le domaine de la protection des données d'applications et de prestations de service. Sur son site Internet, l'institut AV-Test met régulièrement à la disposition du public les tests les plus récents et des résultats de recherches actuels.

Lien : **www.av-test.org/fr**

#3 Une alternative à SecureDrop

AVEC TUTANOTA

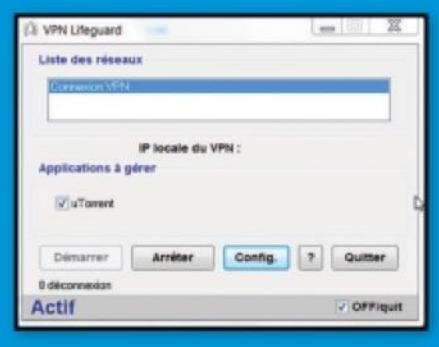
Nous vous avions déjà parlé du service Tutanota et nous avions même interviewé ses créateurs dans notre numéro 35. Rappelons que ce Webmail basé en Allemagne propose un chiffrement de bout en bout en local. Tout le processus de chiffrement se fait depuis chez vous, sur votre navigateur sans risque d'interception. Mais ce qui nous intéresse ici c'est la nouvelle fonctionnalité de formulaire de contact sécurisé. De quoi s'agit-il ? Ce «secure contact form» permet à n'importe qui de vous envoyer des messages chiffrés sur votre boîte aux lettres Tutanota via un formulaire à implémenter sur un site (le vôtre par exemple). Le concept n'est pas nouveau et c'est d'ailleurs ce que propose le site SecureDrop, mais si vous êtes déjà utilisateur de Tutanota, cette fonctionnalité est très facile à jouter pour n'importe quelle agence de presse, d'organismes à but non lucratif qui seront en mesure d'ajouter un moyen chiffré et sécurisé de prendre contact avec vous. Plus pragmatiquement, c'est un formidable outil pour que vos clients puissent vous contacter de manière chiffrée sans qu'ils aient un compte Tutanota et sans même rien connaître au chiffrement ! Pour implémenter ce formulaire, il faudra avoir une version premium de Tutanota à 12€/an. Si cette fonctionnalité vous intéresse, jetez un œil au chapitre 2.3.7 de cette page : https://tutanota.com/how-to.



Lien : **https://tutanota.com**

#4 Sécurisez votre VPN

avec VPN Lifeguard



En cas de déconnexion intempestive de votre VPN, vous vous retrouvez à découvert, sans forcément vous en rendre compte. VPN Lifeguard détecte la défaillance et coupe les applications qui exploitent la connexion Internet afin d'éviter les fuites. Ces logiciels sont fermés en cas de déconnexion du VPN, puis rechargés dès que la connexion est rétablie. Très utile afin de ne pas être à découvert lors des déconnexions.

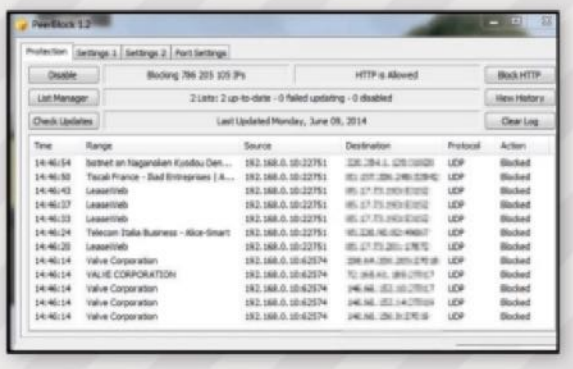
Lien : **https://vpnlifeguard.blogspot.fr**

#5 Filtrage d'IP

avec Peerblock

Peerblock vous permet de contrôler avec qui votre ordinateur dialogue sur Internet, en interdisant certaines adresses IP. Vous pouvez ainsi vous protéger de logiciels dangereux ou indiscrets (adware, spyware, botnet...), ou, en sélectionnant la liste adéquate, vous mettre à l'abri des serveurs qui surveillent votre activité sur les réseaux P2P. Sa mise en œuvre est rapide et aisée et on trouve des listes d'adresses sur Internet.

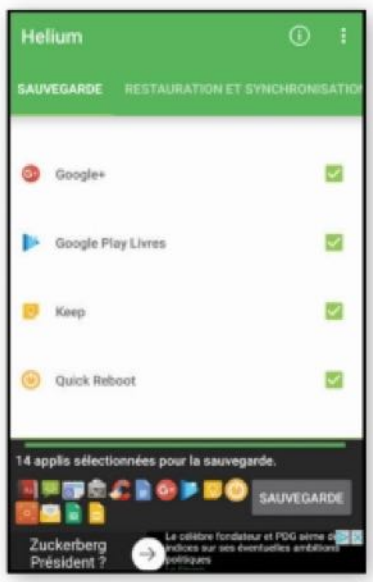
Lien : **https://tinyurl.com/y8w9erx9**



#6 Sauvegarder les données d'applications

avec Helium

Helium sert à sauvegarder en local les données d'applis en tout genre que Google ne gère pas (réseaux sociaux, banque, messagerie...). Installez Helium sur le smartphone depuis le Play Store. Sur le site d'Helium, récupérez le programme de votre choix (ici : l'extension Chrome). Branchez le mobile au PC puis ouvrez l'appli et le programme Helium. Touchez **OK** dans l'appli et attendez la confirmation d'activation. Sur le smartphone, cochez les cases des applications dont vous voulez sauvegarder les données. Touchez la barre verte et faites-la glisser vers le haut ou le bas pour afficher/masquer plus d'options, comme Tout sélectionner. Une fois vos choix effectués, appuyez sur Sauvegarde puis Stockage Interne (la sauvegarde sur le Cloud nécessite la version payante d'Helium). Sur le PC, explorez le mobile et copiez le dossier **carbone,** puisqu'il sera perdu lors d'un root par exemple. Il faudra alors réinstaller l'application Helium, placer le dossier **carbone** à la racine du smartphone, puis ouvrir l'appli, aller dans **Restauration et synchronisation > Stockage Interne**, cocher les cases souhaitées et valider avec **Restaurer**.

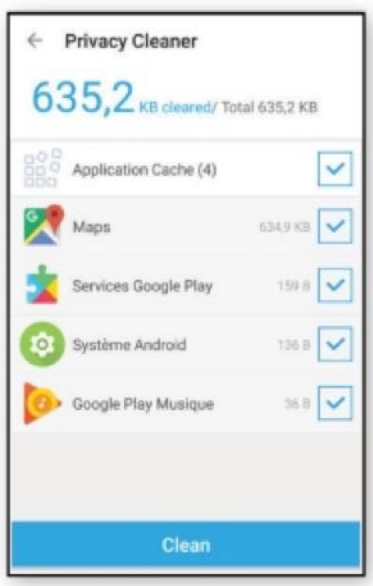


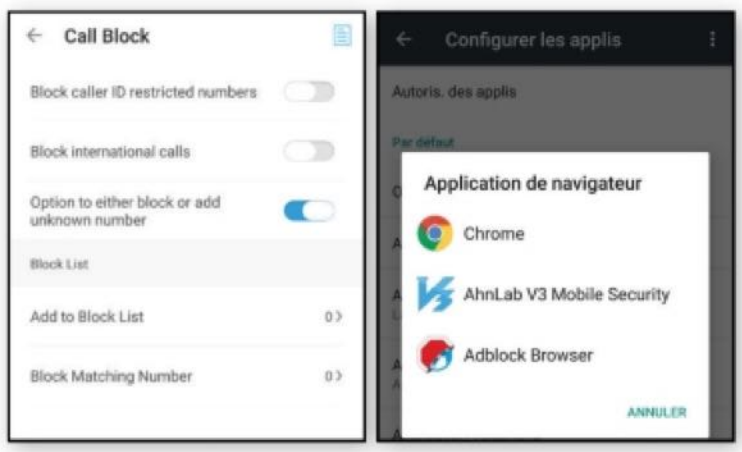
Lien : **https://tinyurl.com/bdkpewo**

#7 Une protection efficace pour mobile

avec AhnLab V3 Mobile Security

Si vous installez des applications Android qui ne viennent pas du Play Store vous prenez le risque de chopper un malware sur votre smartphone. Heureusement AhnLab vous protège gratuitement et ajoute des fonctionnalités sympas comme le nettoyeur de trace. Ouvrez le menu hambruger (les trois traits parallèles) et touchez **Privacy Cleaner**. L'application cherche sur votre appareil toutes les traces potentiellement sensibles laissées par les applications. On trouve aussi un bloqueur d'appel (**Call Block**) et un **scan d'URL** permettant de scanner les liens et les QR codes rencontrés lors de votre navigation sur le Web, pour s'assurer qu'ils ne renvoient pas vers des programmes malveillants. AhnLab peut être assez intrusif si vous laissez les paramètres par défaut. Dans **Settings**, décochez par exemple les cases **Status Bar Icon**, **Get notification even when app is safe** et **Recommend features to use**. L'antimalware se fera plus discret. Si vous êtes rooté et/ou si vous avez autorisé l'installation d'applications de sources inconnues, décochez **Unknown sources** et **Rooting** pour ne plus recevoir d'avertissement inutile.





Lien : **https://goo.gl/gaqyDt**

NOUVEAU !

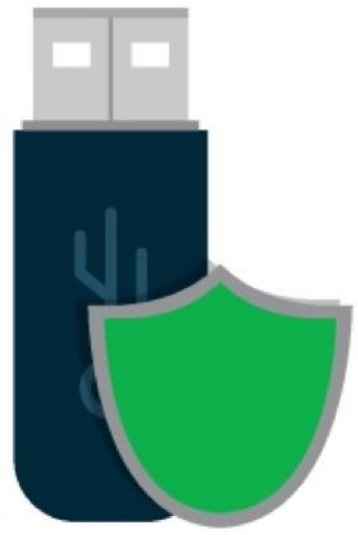
Par l'équipe de *Pirate Informatique* !

L'officiel PC
RASPBERRY PI
Idées & Projets Clés en Main

GUIDE COMPLET

CHEZ VOTRE MARCHAND DE JOURNAUX

CRÉER SA CLÉ USB CHIFFRÉE AVEC VERACRYPT !



Mis au point par la société française IDRIX, VeraCrypt propose de chiffrer un volume ou une partition pour y placer des fichiers sensibles. Dans cet article nous verrons comment créer un conteneur chiffré sur une clé USB ou un disque dur externe. Notez que VeraCrypt est compatible avec les conteneurs de TrueCrypt, vous pouvez donc passer à cette nouvelle solution qui corrige aussi une faiblesse de ce logiciel.

VeraCrypt est né suite à une étude sur TrueCrypt demandée par un client de IDRIX en 2012. Cette étude n'a pas trouvé de problème de sécurité majeur (une faiblesse connue concernant la dérivation de clé de chiffrement). C'est ce dernier point qui a poussé Mounir Idrassi à concevoir VeraCrypt comme un «fork» de TrueCrypt. Le but était de remédier à ce défaut en augmentant le niveau de sécurité face aux attaques par force brute qui sont devenues très performantes. Ainsi, la première version de VeraCrypt a été publiée le 22 juin 2013 sur Sourceforge et Codeplex, un an avant l'arrêt brutal du projet TrueCrypt. Car TrueCrypt n'est plus ! Le logiciel de chiffrement gratuit et open source n'est plus disponible et plus mis à jour depuis 4 ans. Non seulement VeraCrypt sera à même d'utiliser vos anciens conteneurs, mais il présente des améliorations indispensables. Suivez le guide et n'oubliez pas de faire un don si vous utilisez le logiciel...

Quoi de mieux qu'une clé USB *«Pirate Informatique»* pour placer un volume chiffré ? Si votre clé USB ou disque dur n'est pas vierge vous pouvez choisir l'option Encrypted partition in place lorsqu'elle vous sera proposée. Le processus sera un peu plus long.

PAS À PAS

Fonctionnement de VeraCrypt 1.22

CE QU'IL VOUS FAUT

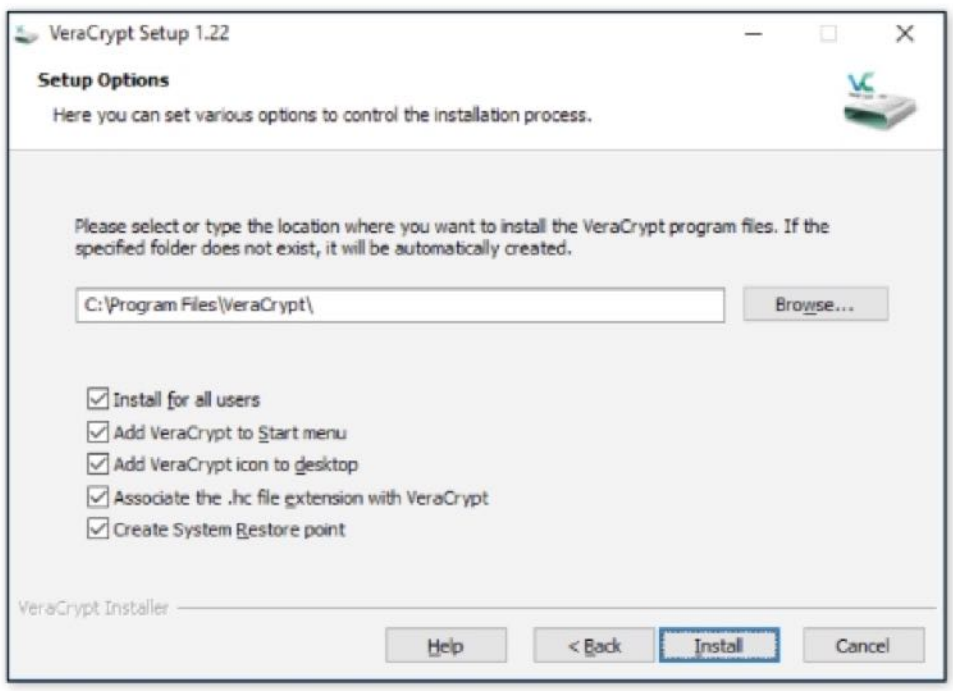
VERACRYPT

OÙ LE TROUVER ? :
http://sourceforge.net/projects/veracrypt

DIFFICULTÉ :

01 L'INSTALLATION

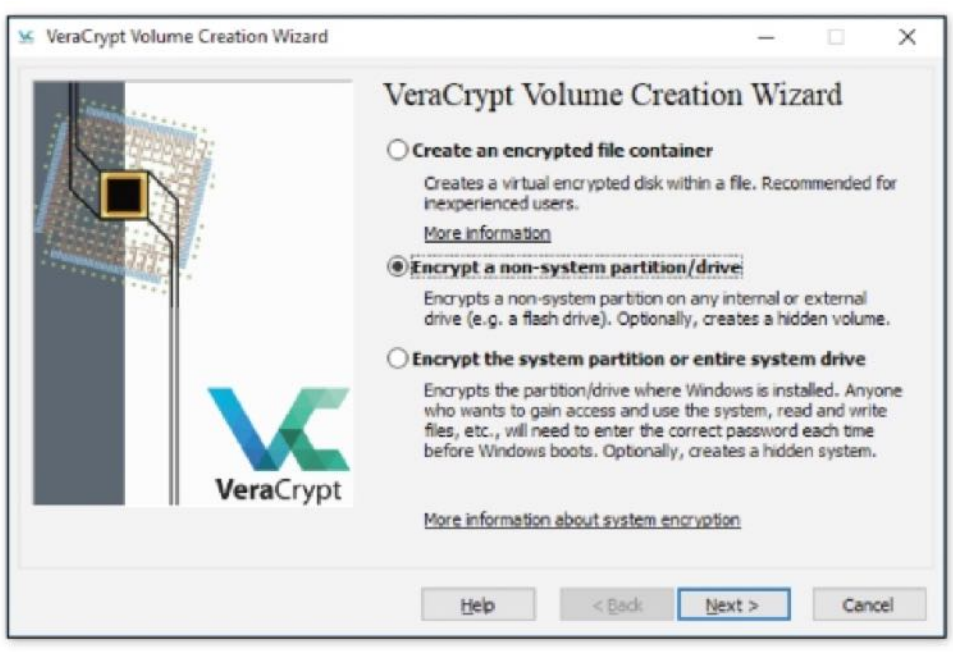
Lors de l'installation, choisissez **Install** au lieu de **Extract**. Cette deuxième option permet de placer les fichiers nécessaires à l'exécution de VeraCrypt sur une clé USB pour l'utiliser chez un ami en mode «portable». Dans les **Setup Options**, laissez



toutes les cases cochées (sauf la dernière si vous ne souhaitez pas créer de point de restauration). La fenêtre principale va alors s'afficher. Notez que vous pouvez changer la langue an allant dans **Settings>Langages...**

02 LES TROIS OPTIONS

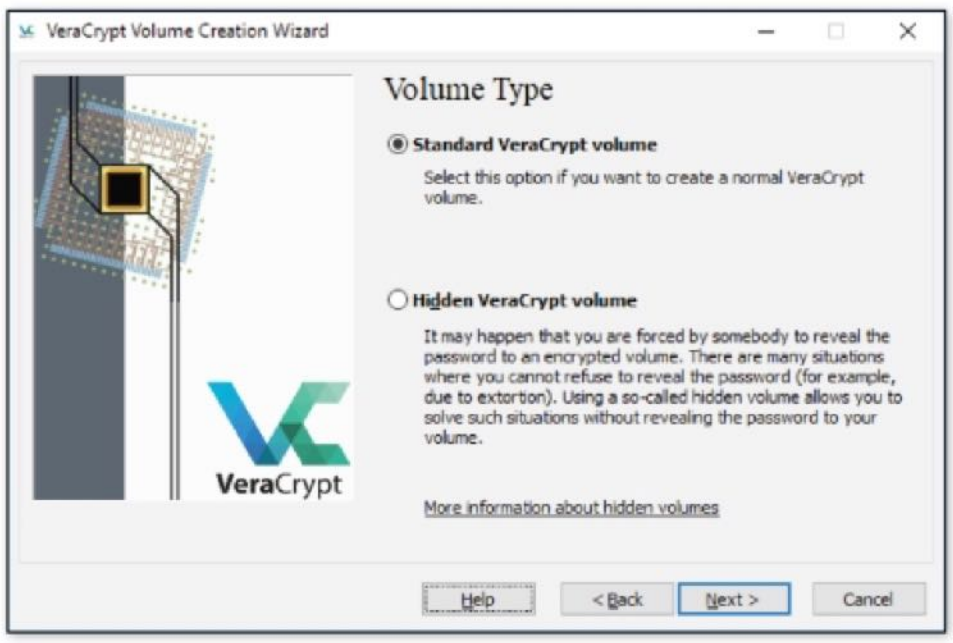
Dans la fenêtre principale du logiciel, cliquez sur **Create Volume**. Vous aurez, ici, trois options. La première consiste à



créer un volume chiffré dans un fichier. La deuxième permet de chiffrer toute une clé USB ou disque dur externe non-système (c'est la solution que nous sélectionnerons). La dernière permet de chiffrer tout le disque dur principal (contenant Windows). Avec cette option, il est même possible de créer un système caché.

03 VOLUME STANDARD OU CACHÉ ?

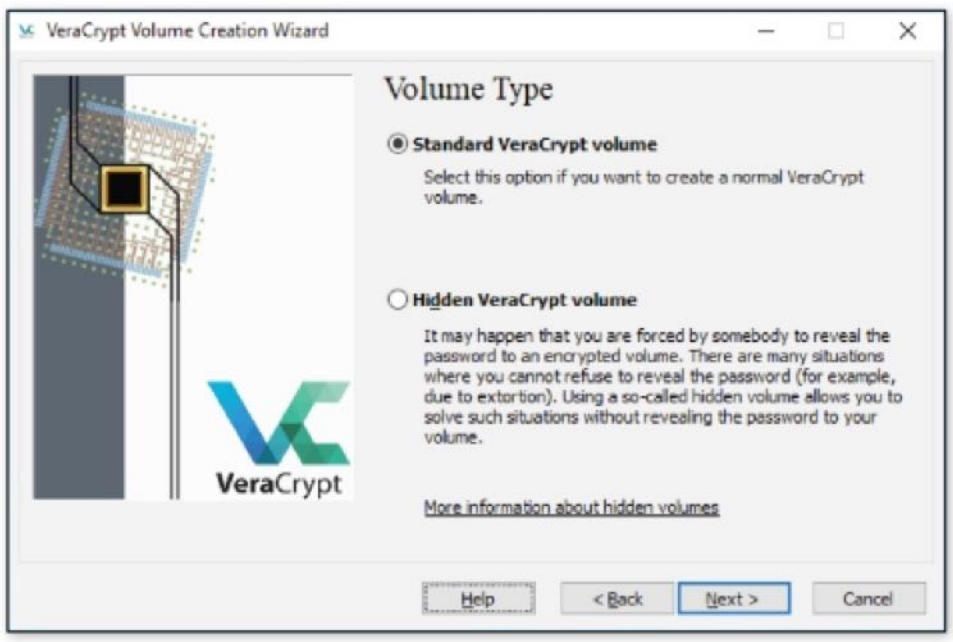
Nous choisissons la deuxième option pour chiffrer complètement une clé USB, par exemple. Après validation, le logiciel demande si



nous souhaitons créer un volume chiffré standard ou un volume caché (pour utiliser le «déni plausible» en cas de torture ou de chantage). Comme nous ne sommes pas du KGB et que notre clé ne contient que des informations non sensibles, nous allons choisir la première option...

04 CRÉATION DU VOLUME

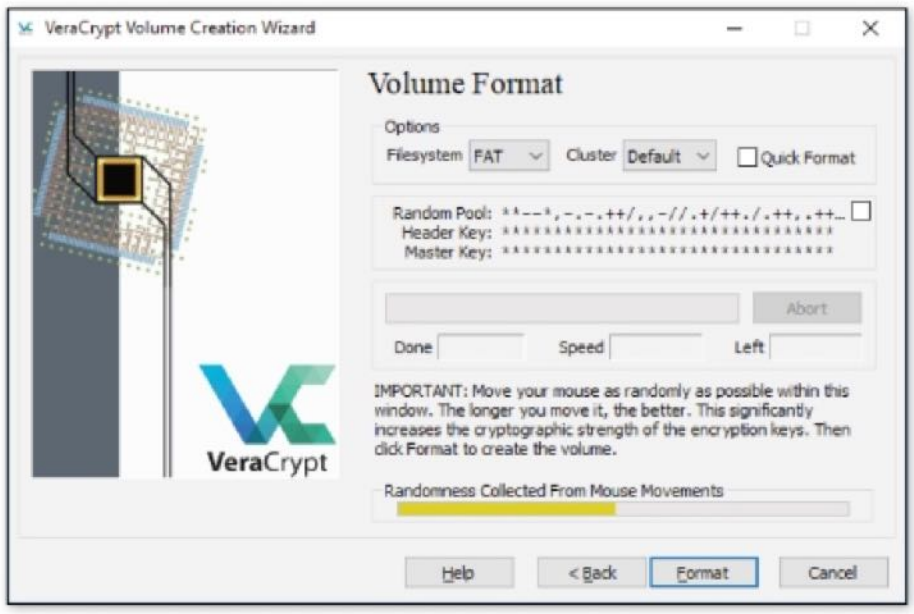
Sélectionnez ensuite une partition ou un périphérique. Le logiciel vous donne le choix entre créer le volume chiffré et le formater ou chiffrer les données qui sont déjà installées (ne fonctionne qu'en NTFS). Après avoir choisi la première option



(plus simple, car notre clé est vide et en FAT32), le logiciel vous demandera quel algorithme vous désirez utiliser. Laissez AES dans le doute, mais vous pouvez aussi opter pour un chiffrement en cascade avec pas moins de trois algorithmes les uns sur les autres comme Twofish ou Serpent (deux finalistes du concours AES de 2000)

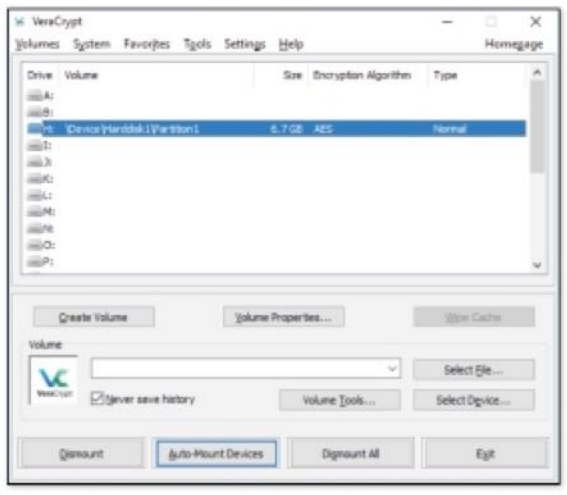
05 LE FORMATAGE

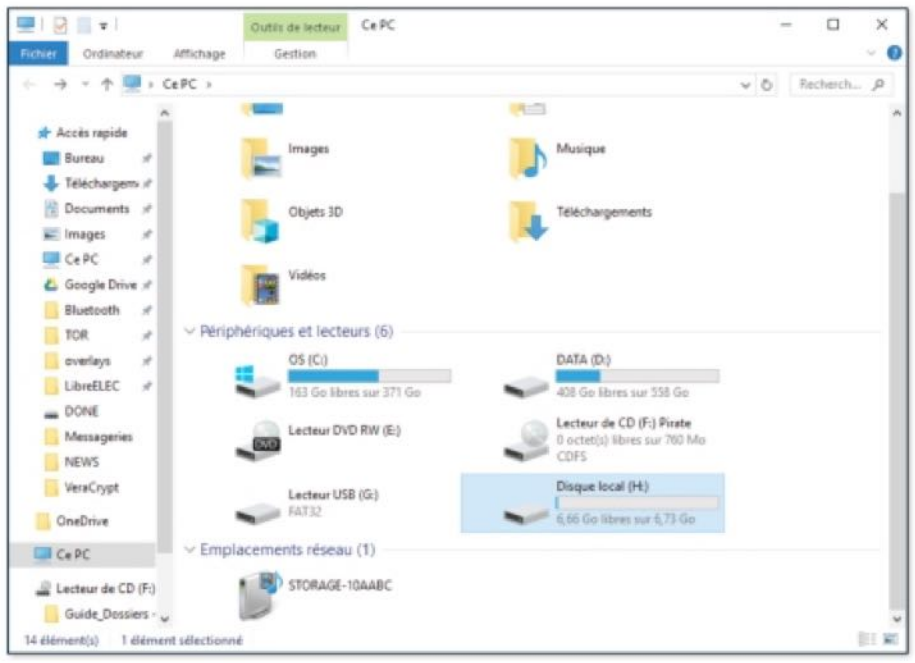
Validez encore deux fois et choisissez votre mot de passe. Il est possible de créer un fichier clé au cas où vous oublieriez votre mot de passe. Ce dernier peut prendre la forme d'un MP3 ou de n'importe quel autre fichier (son contenu ne sera pas modifié). Après validation, VeraCrypt va vous demander si vous souhaitez mettre des fichiers de plus de 4Go. Dans ce cas, le logiciel choisira automatiquement un formatage NTFS au lieu du classique FAT32. Cliquez sur **Format** après avoir bougé la souris aléatoirement dans la fenêtre pour générer la clé de cryptage.



06 LE MONTAGE

À la fin du processus (qui peut durer de longues minutes), faites **Exit** et, dans l'interface principale du logiciel, sélectionnez une lettre de lecteur, cliquez sur **Auto-Mount Device** et tapez votre mot de passe. Vous verrez alors que votre clé USB a changé de lettre (ici H au lieu de G). L'ancienne lettre est toujours présente, mais ne sera plus active. Dans **Ordinateur**, vous avez accès au disque local G après insertion et validation du mot de passe. Mettez-y tous vos fichiers sensibles. Faites **Dismount All** pour les rendre inaccessibles. Attention, car même si vos données sont protégées, elles peuvent être effacées.

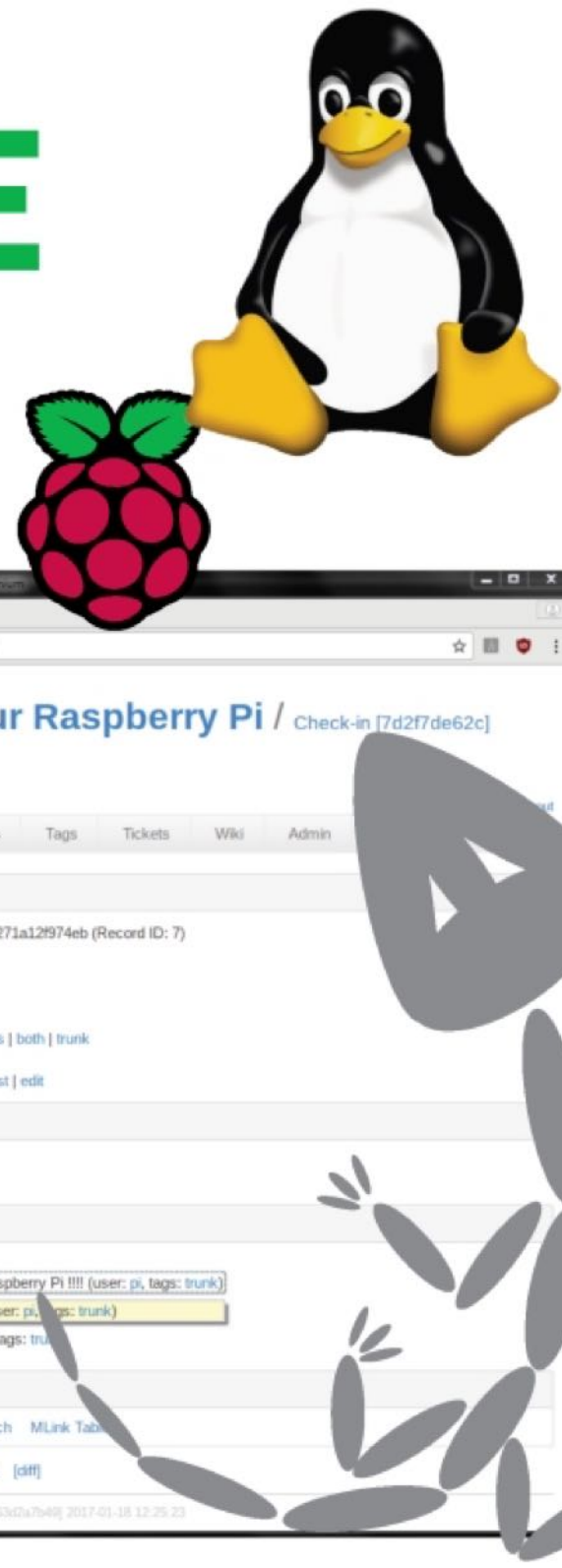




« Aujourd'hui, la vie numérique est une part essentielle de notre existence et notre patrimoine personnel, les biens numériques ayant la même valeur que les biens physiques. De ce fait, il convient donc de les protéger des intrusions et des vols au travers de l'utilisation du chiffrement, ce qui est tout aussi naturel que l'utilisation de cadenas pour les valises et de serrures pour les portes. Ceci devient encore plus important quand on utilise le Cloud pour stocker ses données numériques: cela équivaut à mettre ses affaires dans un entrepôt où tout naturellement on va poser cadenas et verrous pour les protéger. Mais il est clair que la démocratisation des solutions de chiffrement comme VeraCrypt provoque la nervosité des services de renseignements... »

- Mounir Idrassi, PDG de IDRIX et créateur de VeraCrypt -

FOSSIL : UNE ALTERNATIVE SÉRIEUSE À GIT



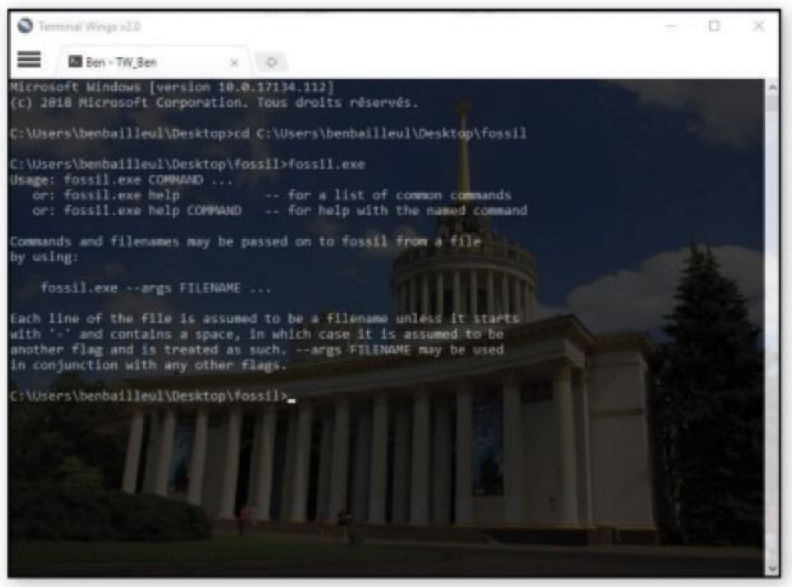
Fossil est un logiciel de «gestion de versions» ce qui signifie qu'il va accompagner et garder trace pour vous des ajouts, modifications ou suppressions des (ou dans les) fichiers que vous lui ferez surveiller. Son utilité apparaît dès lors que l'on recherche un suivi dans la rédaction de document, de code source, etc. C'est une alternative sérieuse à Git tout en apportant quelques ajouts fort intéressants ...

Merci à Marc Delb pour son article !

LEXIQUE

***PATH :**
PATH est une variable d'environnement sous Linux et d'autres systèmes d'exploitation de type Unix qui indique au shell sur quels répertoires rechercher des fichiers exécutables en réponse aux commandes émises par un utilisateur. Pour en savoir plus, nous vous conseillons cette lecture : **https://tinyurl.com/ybq5dclr.**

Fossil a fait le choix de la simplicité. En effet, son installation consiste à copier un exécutable dans un emplacement connu par la variable système PATH et c'est tout ! Il est aussi disponible (binaires ou source) sous Linux, MacOS, OpenBSD et Windows. Il intègre un site Web «clé en main» dédié à votre projet ainsi qu'un Wiki et un traqueur de bogues. Notez également que ce site Web est justement une application directe (ainsi qu'une vitrine) des possibilités de Fossil puisqu'il s'agit de l'interface Web dédiée au contrôle de version du projet Fossil lui-même ! Pour changer un peu nos habitudes, nous avons décidé de faire ce tuto avec un Raspberry Pi sous Raspbian, que vous commencez à connaître si vous nous lisez. Bien sûr, cela fonctionne de la même manière sur d'autres distributions dérivées de Debian comme Ubuntu. Sous Windows, nous vous conseillons d'utiliser le logiciel en ligne de commande avec Terminal Wings de la société Phrozen.



PAS À PAS

Fossil : les grands principes

CE QU'IL VOUS FAUT

FOSSIL

OÙ LE TROUVER ? :
http://fossil-scm.org

DIFFICULTÉ :

01 L'INSTALLATION

Sous Raspbian, nous pouvons utiliser la manière classique d'installation (après avoir mis à jour les dépôts) :

```
pi@raspi-16Go-1:~ $ sudo apt-get update -y && sudo apt-get upgrade -y
Hit:1 http://mirrordirector.raspbian.org/raspbian stretch InRelease
Hit:2 http://archive.raspberrypi.org/debian stretch InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
pi@raspi-16Go-1:~ $ sudo apt-get install fossil
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  fossil
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/586 kB of archives.
After this operation, 1,739 kB of additional disk space will be used.
Selecting previously unselected package fossil.
(Reading database ... 123461 files and directories currently installed.)
Preparing to unpack .../fossil_1%3a1.37-1_armhf.deb ...
Unpacking fossil (1:1.37-1) ...
Setting up fossil (1:1.37-1) ...
Processing triggers for man-db (2.7.6.1-2) ...
pi@raspi-16Go-1:~ $
```

sudo apt-get update -y && sudo apt-get upgrade –y
sudo apt-get install fossil

Fossil est maintenant installé. Prenons l'exemple de ce code source indispensable à la vie harmonieuse de tout programmeur et que nous ferons suivre par Fossil : j'ai nommé le fameux *Hello World*, bien entendu !

02 CRÉATION DU DÉPÔT

Commençons par créer un dépôt Fossil avec :
fossil init Hello.fossil

```
pi@raspi-16Go-1:~/devel/Hello $ fossil init Hello.fossil
project-id: f15832ab099abc52201e82d6358648509ec128a1
server-id:  1d7a61e2bc37829eff98eb78d22e1c1c68628676
admin-user: pi (initial password is "beb2bb")
pi@raspi-16Go-1:~/devel/Hello $ ll
total 216K
-rw-r--r-- 1 pi pi  132 Dec 31 04:54 hello.cpp
-rw-r--r-- 1 pi pi 212K Dec 31 05:04 Hello.fossil
pi@raspi-16Go-1:~/devel/Hello $
```

Les commandes à saisir sont presque identiques, dans leurs usages et dans beaucoup de leurs mots-clés, à celles de Git.

03 OUVERTURE DU DÉPÔT

Ce dépôt **Hello.fossil** est une base de données qui contiendra par la suite toutes les informations nécessaires à l'examen des différences qui apparaîtront dans le code source. Lors de sa création, le dépôt n'est pas ouvert par défaut et nous devons saisir :
fossil open Hello.fossil

Ajoutons au dépôt le fichier à suivre avec :
fossil add hello.cpp

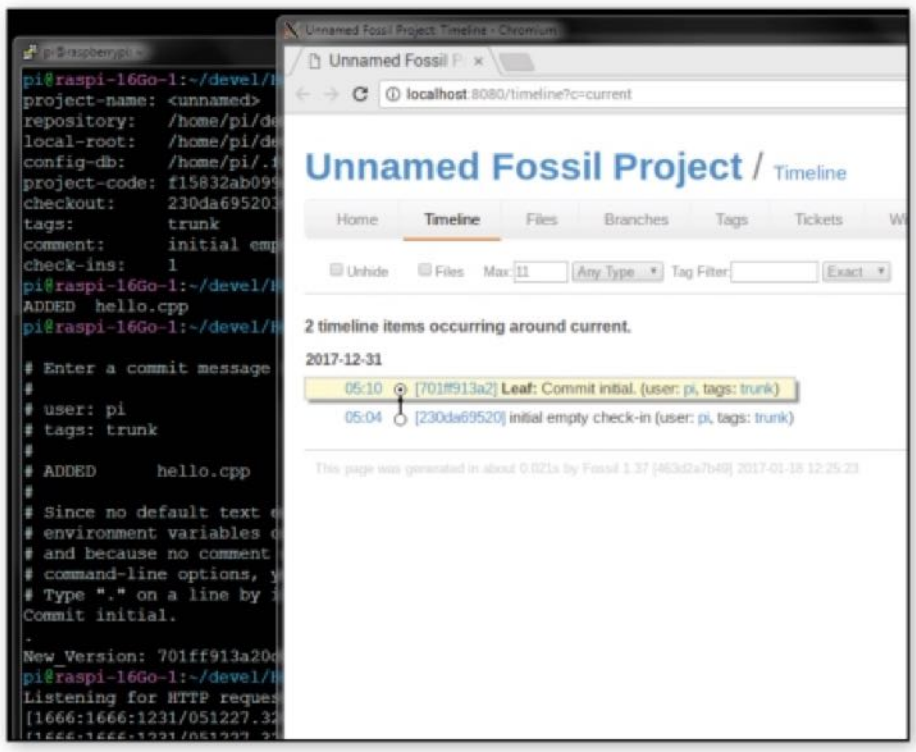
Enregistrons l'état initial du code source contenu dans **hello.cpp** avec :
fossil commit

```
pi@raspi-16Go-1:~/devel/Hello $ fossil open Hello.fossil
project-name: <unnamed>
repository:   /home/pi/devel/Hello/Hello.fossil
local-root:   /home/pi/devel/Hello/
config-db:    /home/pi/.fossil
project-code: f15832ab099abc52201e82d6358648509ec128a1
checkout:     230da6952034728e322fd16d25bab87566a28226 2017-12-31 05:04:25 UTC
tags:         trunk
comment:      initial empty check-in (user: pi)
check-ins:    1
pi@raspi-16Go-1:~/devel/Hello $ fossil add hello.cpp
ADDED  hello.cpp
pi@raspi-16Go-1:~/devel/Hello $ fossil commit

# Enter a commit message for this check-in. Lines beginning with # are ignored.
#
# user: pi
# tags: trunk
#
# ADDED      hello.cpp
#
# Since no default text editor is set using EDITOR or VISUAL
# environment variables or the "fossil set editor" command,
# and because no comment was specified using the "-m" or "-M"
# command-line options, you will need to enter the comment below.
# Type "." on a line by itself when you are done:
Commit initial.
.
New_Version: 701ff913a20d0c5536600cd69c638d7bd866ddc9
pi@raspi-16Go-1:~/devel/Hello $ fossil ui
```

Il nous est alors demandé d'ajouter un message qui servira de «référence» à cet enregistrement (le texte **Commit initial.** en l'occurrence).

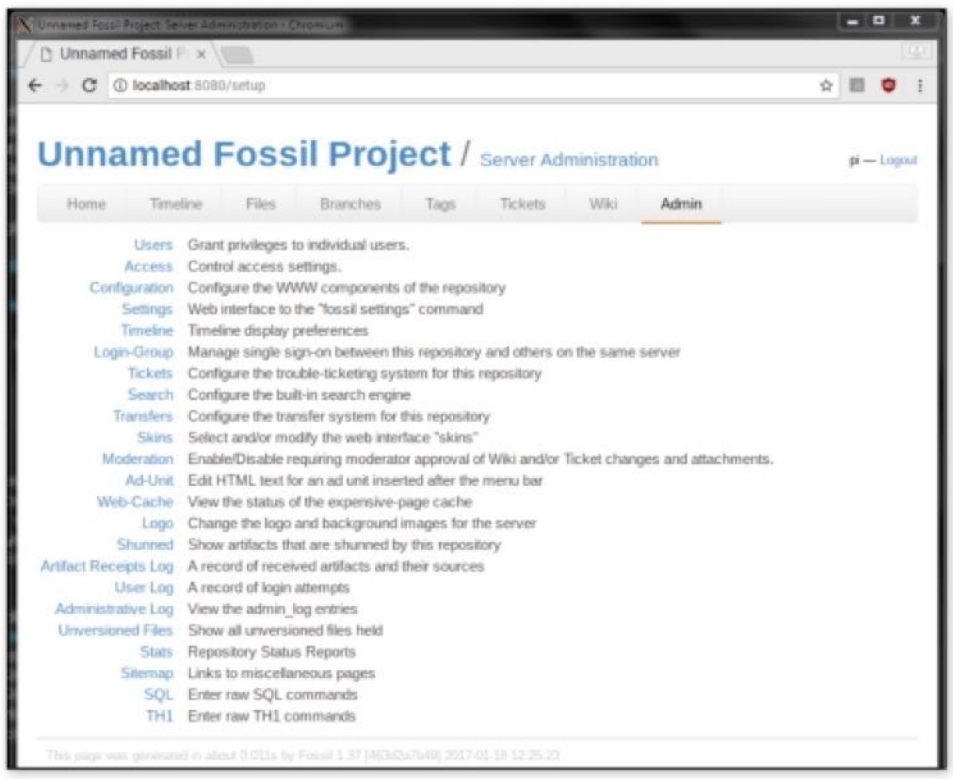
04 L'IDENTIFIANT UNIQUE

Le message **New_Version** est affiché et le nombre hexadécimal qui le suit est un identifiant unique de la version du fichier à cet instant précis… La dernière commande (**fossil ui**) dans la copie d'écran précédente, invoque l'interface graphique dédiée au projet dans le navigateur Web par défaut.



05 LA TIMELINE

On peut retrouver visuellement dans la Timeline (le suivi de toutes les opérations en rapport avec notre projet) le check-in initial (la création du dépôt) et notre premier **commit** (ou étape



de développement). Cependant, l'aspect visuel ne s'arrête pas à la Timeline mais révèle aussi par le biais des différents onglets de nombreuses possibilités d'exposition du projet. Il faudra passer par une étape de configuration rapide via l'onglet **Admin**...

06 PERSONNALISATION DE LA PAGE

Ici vous pourrez indiquer le nom du projet et personnaliser un peu plus la page depuis l'onglet Wiki).
Il est temps de revenir à notre code source et de lui apporter quelques modifications de bon aloi, à commencer par une traduction française !

```
pi@raspberrypi: ~
  GNU nano 2.7.4
#include <iostream>

using namespace std;


int main(int argc, char* argv[])

{

  cout << "Bonjour le Monde !" << endl;

  return 0;

}
```

07 NOUVELLE MODIFICATION DU CODE

```
pi@raspi-16Go-1:~/devel/Hello $ nano hello.cpp
pi@raspi-16Go-1:~/devel/Hello $ fossil commit

# Enter a commit message for this check-in. Lines beginning with # are ignored.
#
# user: pi
# tags: trunk
#
# EDITED    hello.cpp
#
# Since no default text editor is set using EDITOR or VISUAL
# environment variables or the "fossil set editor" command,
# and because no comment was specified using the "-m" or "-M"
# command-line options, you will need to enter the comment below.
# Type "." on a line by itself when you are done:
Traduction française.
.
New_Version: 7d2f7de62c4769fff6ab31d436f2271a12f974eb
pi@raspi-16Go-1:~/devel/Hello $
```

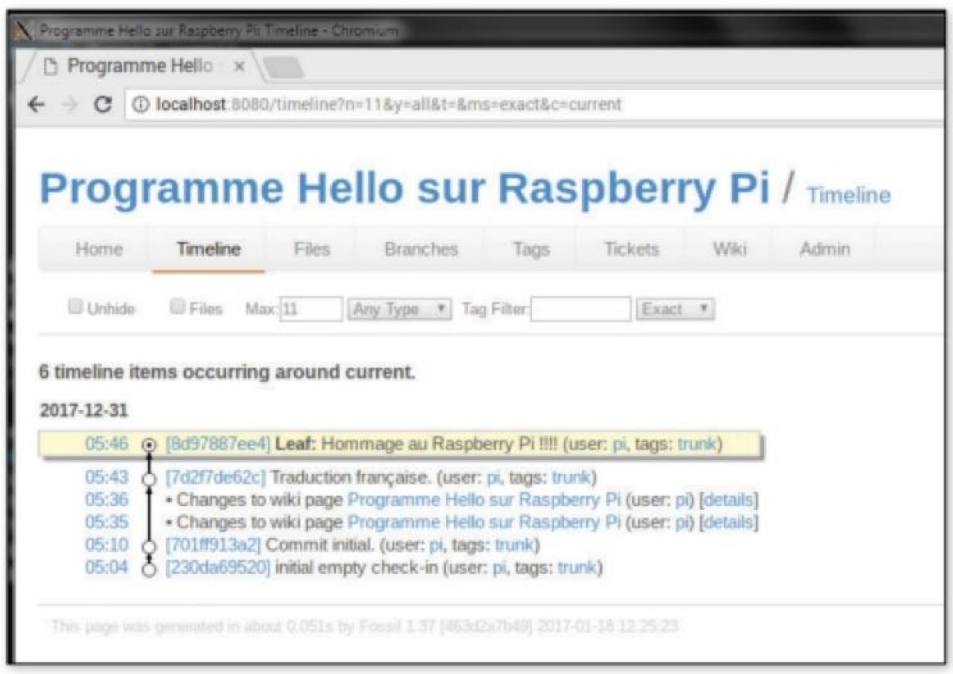
Intégrons cette modification dans le dépôt avec **fossil commit** et ajoutons le message descriptif de cette nouvelle version. Allons plus loin dans l'usage de la langue française et profitons-en pour rendre un hommage appuyé à la Framboise ! Ajoutons

```
pi@raspi-16Go-1:~/devel/Hello $ fossil commit

# Enter a commit message for this check-in. Lines beginning with # are ignored.
#
# user: pi
# tags: trunk
#
# EDITED    hello.cpp
#
# Since no default text editor is set using EDITOR or VISUAL
# environment variables or the "fossil set editor" command,
# and because no comment was specified using the "-m" or "-M"
# command-line options, you will need to enter the comment below.
# Type "." on a line by itself when you are done:
Hommage au Raspberry Pi !!!!
.
New_Version: 8d97887ee4c2e67a926f0332cc7656d3919827bb
pi@raspi-16Go-1:~/devel/Hello $
```

une nouvelle modification du code source avant de faire un nouveau commit.

08 L'HISTORIQUE DES MODIFICATIONS

L'utilité principale du suivi de projet est de pouvoir revenir sur l'historique de toutes les modifications que nous avons apportées (aussi bien en ce qui concerne le code source que

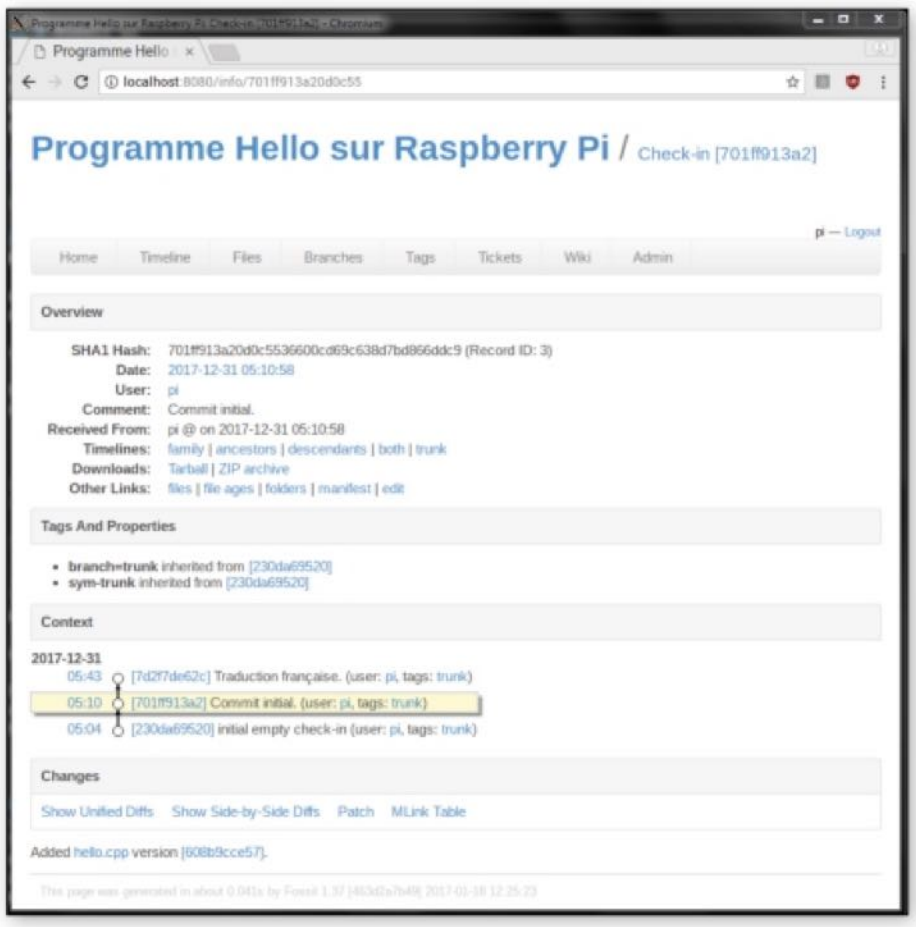


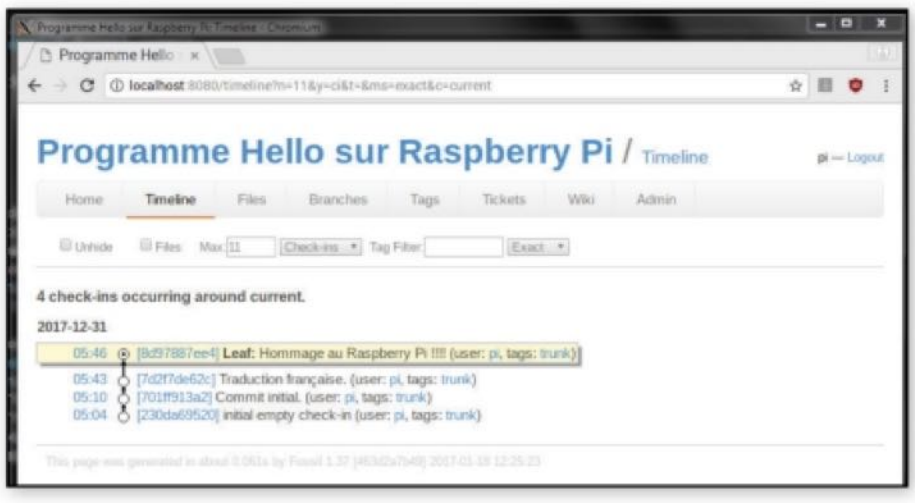
```
pi@raspberrypi: ~
  GNU nano 2.7.4
#include <iostream>

using namespace std;


int main(int argc, char* argv[])

{

  cout << "Bonjour le Monde du Raspberry Pi !" << endl;

  return 0;

}
```

l'édition du wiki de la page d'accueil), il suffit d'afficher l'onglet Timeline à nouveau, et d'éventuellement filtrer sur les entrées qui nous intéressent. Tous les commits du code source par exemple (check-ins).

09 RETOUR À UN ÉTAT ANTÉRIEUR

Il est possible de revenir à un état antérieur des modifications du code source en sélectionnant le numéro d'enregistrement unique en hexadécimal en regard de tous les commits. On peut aussi télécharger le fichier modifié à cet état précis du développement via les liens Tarball ou Zip archive. Il est aussi possible d'avoir un simple aperçu du fichier.

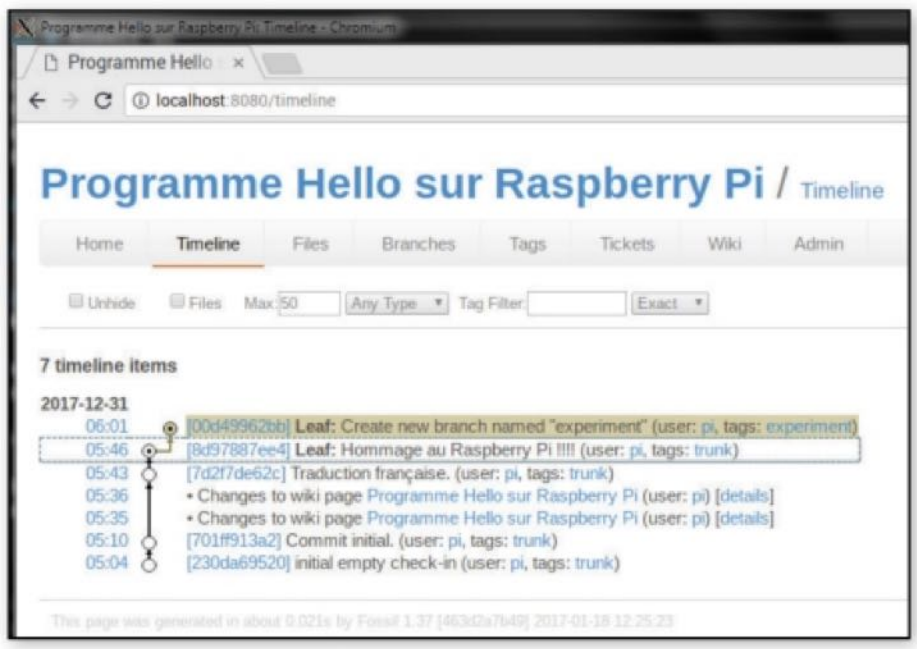




10 JONGLER AVEC LES «BRANCHES»

On peut aisément changer de commit, retrouver par exemple la traduction française de notre projet en suivant la même procédure de sélection de l'identifiant unique du commit et obtenir l'aperçu du code source qui nous intéresse… À l'instar de Git, il est tout aussi aisé de créer des branches. Une branche permet un développement en parallèle d'un projet (sans affecter le «tronc»).

Le plus souvent utilisée pour ajouter (et tester) de nouvelles fonctionnalités au projet, la branche expérimentale peut être fusionnée (**merge**) à la branche principale. De la même manière, des tags (balises) peuvent être ajoutés pour marquer un moment spécifique du développement (versions de production par exemple). Fermons le navigateur et arrêtons le serveur Web embarqué en faisant **Ctrl**+**C** (il s'agit de la procédure normale). Sans oublier la dernière commande **fossil close** pour refermer le dépôt. Pour désinstaller Fossil, vous pouvez saisir **sudo apt-get autoremove --purge fossil**




```
pi@raspberrypi: ~
pi@raspi-16Go-1:~/devel/Hello $ ll
total 4.0K
-rw-r--r-- 1 pi pi 132 Dec 31 04:54 hello.cpp
pi@raspi-16Go-1:~/devel/Hello $ cat hello.cpp
#include <iostream>

using namespace std;


int main(int argc, char* argv[])

{

  cout << "Hello World !" << endl;

  return 0;

}
pi@raspi-16Go-1:~/devel/Hello $
```

0101001010010101010010000111010101010101101010100010011010

CLONAGE RFID :

« QUI VOLE UN CAFÉ, VOLE UNE BMW ! »

LEXIQUE

***RFID :**
RFID est le sigle de Radio Frequency Identification (ou radio-identification dans la langue de Sébastien Cauet). Il s'agit d'une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés tag RFID ou «radio-étiquettes». Ceux-ci sont souvent sous la forme d'étiquettes autocollantes, mais on peut en trouver dans de très petits objets. Il comprennent une antenne associée à une puce électronique qui leur permet de recevoir et de répondre aux requêtes radio émises depuis un émetteur-récepteur (smartphone, ordinateur ou machine à café dans ce cas de figure).

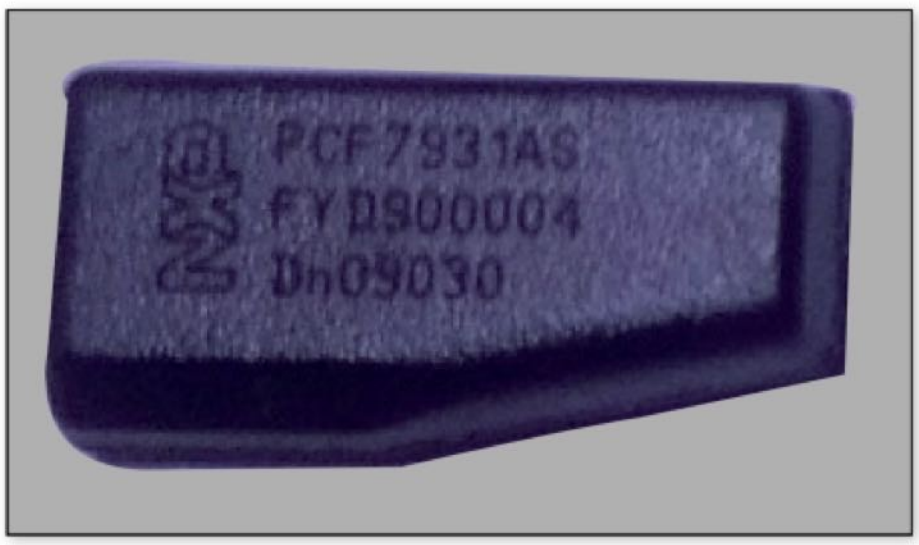
Après s'être attaqué aux fontaines à soda de chez KFC et aux vignettes Crit'air, notre camarade The LoneGunman s'est penché sur les machines à café qui prennent place dans nos bureaux, ateliers ou open spaces, Spoiler alert : il a réussi. Voyons comment...

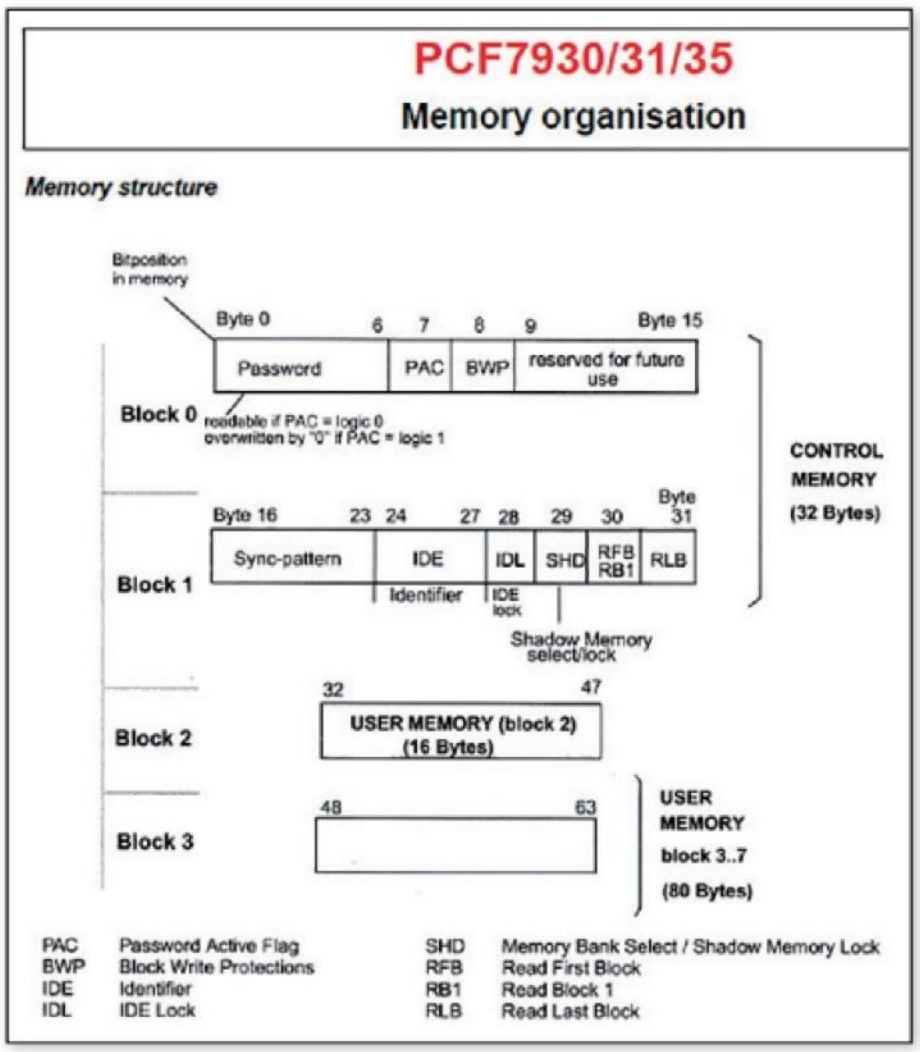
Dans le numéro n° 35, le rédacteur en chef nous a mis au défi de trouver une faille dans le fonctionnement des machines à café professionnelles. Le défi a été accepté, mais dans cet article nous ferons notre possible pour ne pas en dévoiler trop, car l'objectif n'est pas de nuire ni aux fabricants de machines ni aux exploitants de ces machines, et même de mettre en garde les apprentis malandrins. Le but est bien sûr de comprendre le fonctionnement de ce type de « clé café », et de ses failles.

Voici un exemple de clé pour machine à café. Celle-ci fonctionne avec une puce RFID (transpondeur PCF7931AS) du domaine public...

01 LA PUCE

Lorsque nous ouvrons la clé nous pouvons voir grâce à la référence que nous sommes en présence d'une puce RFID (transpondeur PCF7931AS). Cette puce est dans le domaine public et voici un extrait de sa cartographie mémoire.





PCF7930/31/35

Memory organisation

Memory structure

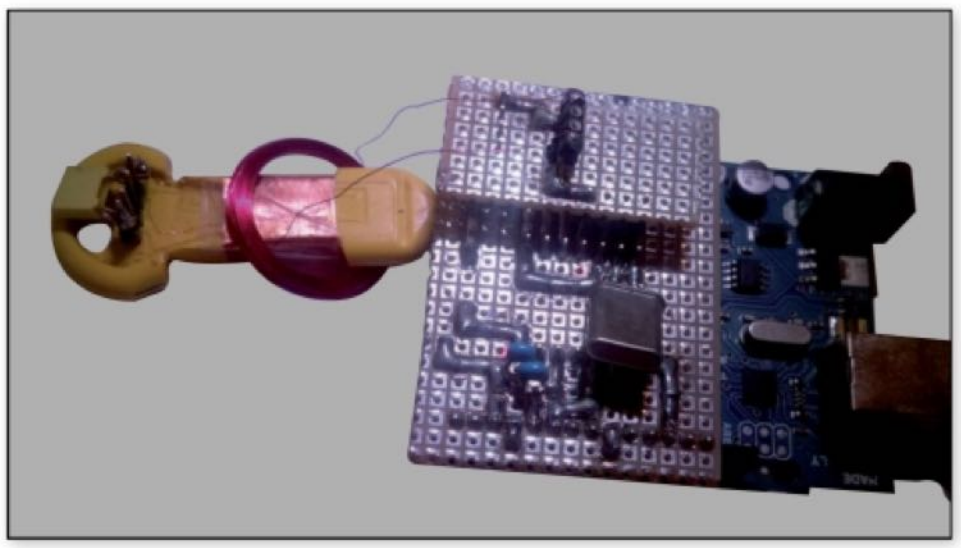
02 LES LIMITES DE L'EXPÉRIENCE

Cette puce est utilisée comme antidémarrage d'un certain nombre de voitures comme chez BMW. L'analyse détaillée de la documentation permet de voir que sans le mot de passe il est impossible d'écrire dans la clé, mais qu'il est possible de la lire. Si plus tard on veut écrire dans la clé on peut déjà noter qu'il ne sera pas possible d'effectuer un brute force sur le mot de passe. Avec 2^56 combinaisons et un «check» toutes les 60ms il nous faudrait 137 millions d'années. Concrètement, la portée de ce genre de transpondeur est centimétrique, on ne peut donc copier son contenu qu'en étant très près. Le contenu de la clé est libre, l'utilisateur, ici BMW, met à l'intérieur ce qu'il veut dans la zone **user** (un identifiant ou autre élément plus compliqué), la copie avec le même **password** permet donc d'avoir un double de la clé de voiture. Ce qui est intéressant, mais pas critique. Cette puce est donc très adaptée pour une clé de voiture. La question est donc comment obtenir le mot de passe pour pouvoir dupliquer ou modifier le contenu de la puce PCF7931As. Pour cela Il va être nécessaire d'analyser les trames électromagnétiques qui passent entre le transpondeur et le lecteur de puce RFID en toute discrétion, pendant une communication légitime avec notre clé. Pour cela on rajoute une spire (un circuit fermé parcouru par du courant électrique) juste à côté de notre puce pour «écouter» ce qui passe comme trame.

03 DUMP DES TRAMES ÉLECTROMAGNÉTIQUES

Pour ce faire, réalisons une antenne pour sniffer les signaux émis par la clé. L'antenne est constituée d'une bobine et d'un condensateur calibré pour résonner à 125khz.

04 LES OUTILS



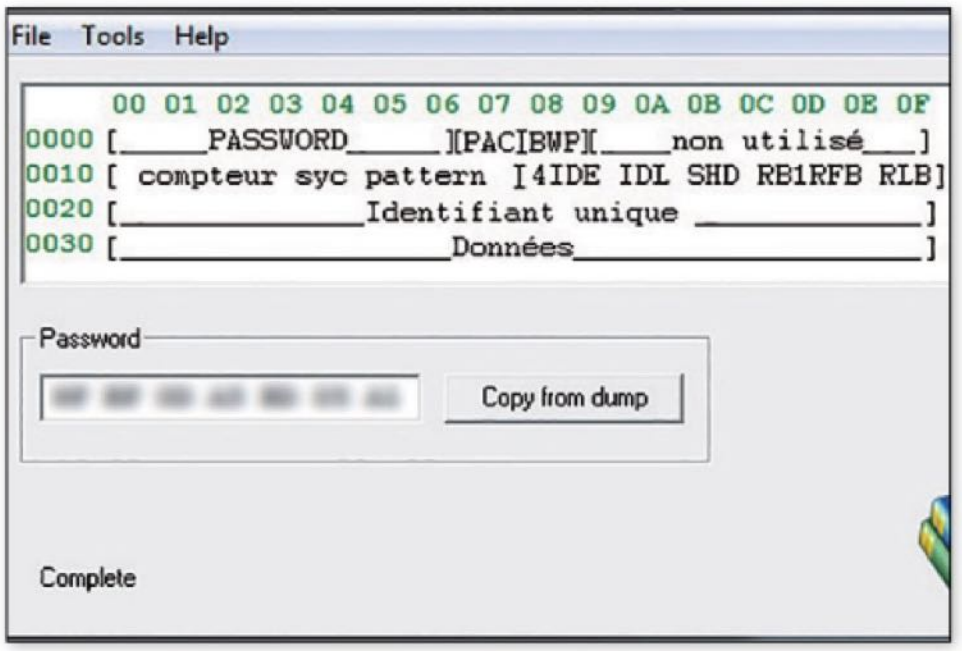
La puce est une puce classiquement utilisée comme anti démarrage, un simple lecteur de clé de voiture ou un circuit à base d'Arduino et de module PCF7991 permet donc la lecture du contenu de la clé. On pourra en profiter en même temps pour analyser les trames électromagnétiques échangées par notre propre puce PCF7931as dont on connaît le mot de passe.

05 LECTURE AVEC LE GAMBIT

La lecture de la puce PCF7930 de la clé café avec le GAMBIT (un appareil permettant de programmer des transpondeurs RFID : https://tinyurl.com/ycu58q2x) donne le résultat suivant (voir la capture). La zone password est à **00 00 00 00 00 00 00**, ceci signifie que la clé est protégée : on peut lire, mais pas écrire.

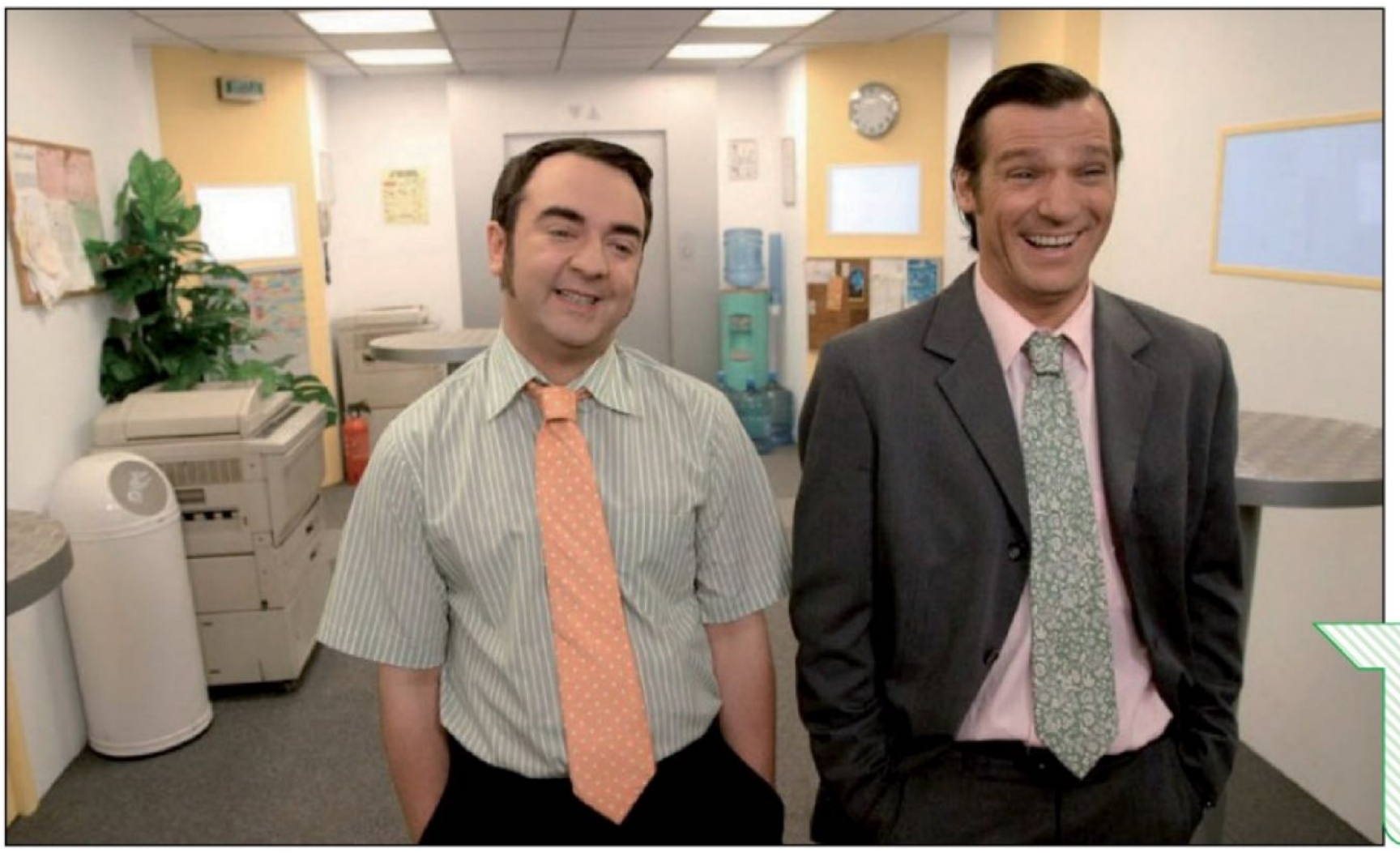
Voici un exemple :
Contenu de la zone user : **0030 55 00 F8 00 F8 AA 00 DC 00 DC 00 00 00 00 00 00**

Ce contenu correspond à une clé avec un solde de 2,20 €, et un solde précédent de 2,48 €. Quand on a fait « Hexa » comme 2ème langue au lycée on voit tout de suite que 2.20 € codé sans la virgule s'écrit 220 en décimal et vaut **00DC** en hexadécimal. On voit aussi que 2.48 € codé sans la virgule s'écrit 248 en décimal et vaut **00F8** en hexadécimal. On retrouve bien **00DC** et **00F8** en double exemplaire entre les balises **55** et **AA**. À ce stade on est donc capable de lire le solde de la clé, mais pas d'écrire dedans. Rien d'exceptionnel, la zone **user** est lisible, ce qui est parfaitement normal.



06 ÉCRIRE SUR NOTRE PROPRE PUCE PCF7931AS

Maintenant que l'on connaît l'encodage, on peut imaginer mettre une somme d'argent différente sur la clé.
Exemple : 59.99 € correspond à 5999 en décimal et correspond

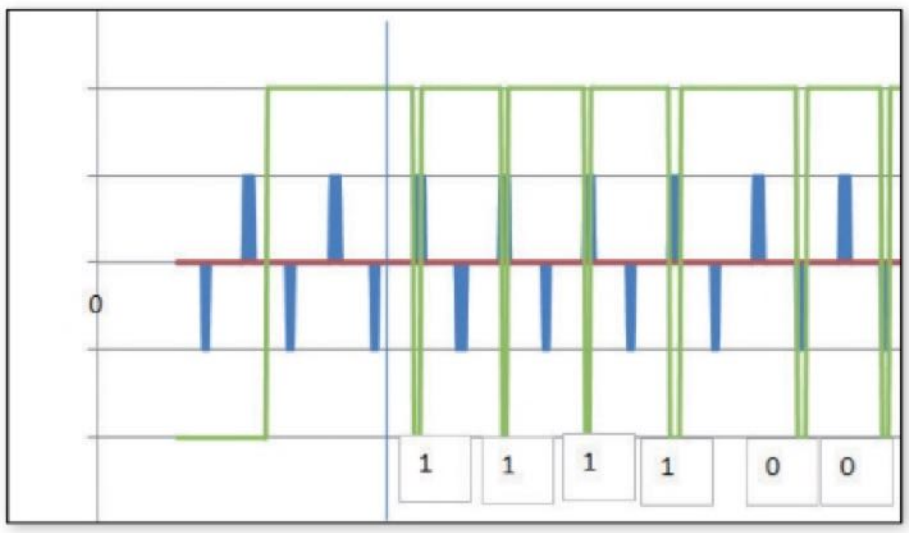


« Un petit café JC ? C'est moi qui invite ! »

à 176F en hexadécimal. Il faudra donc essayer d'écrire avec le GAMBIT : **0030 AA 17 6F 17 6F 55 17 6F 17 6F 00 00 00 00 00 00 00**. Avec notre propre puce achetée sur Internet, et notre propre mot de passe (par exemple **11110000**(...)), on n'a aucun problème avec le GAMBIT à modifier notre puce personnelle. Toutefois, même avec une zone user parfaitement correcte, la BMW, ou la machine à café ne reconnaîtra pas le mot de passe : la clé sera considérée comme invalide et le précieux contenu ne servira à rien. Il nous faut donc absolument trouver le moyen de hacker le password.

07 HACKONS NOTRE PROPRE PUCE PCF7931AS

Essayons de hacker notre propre puce, pour cela il faut sniffer les trames électromagnétiques. Il existe plusieurs techniques, certaines vraiment pas chères et d'autres... beaucoup plus. Nous l'avons déjà dit, mais cet article n'a pas vocation à fournir gratuitement du breuvage aux caféinomanes, mais de comprendre le fonctionnement de ce système de clés. La solution que nous avons retenue est donc une solution chère c'est-à-dire une «solution professionnelle», peu accessible aux communs des mortels. Nous utiliserons un scanner de fréquence décodant le protocole OOK-ASK calibré à la fréquence de 125khz, couplé à un ordinateur pour décoder les trames dont l'antenne est notre spire d'espionnage. On aurait pu utiliser un oscilloscope numérique avec beaucoup de mémoire, et décoder à la main... ou bien un simple téléphone portable... (mais «*chuuut*»). En enregistrant le signal qui passe dans l'air on s'aperçoit très vite que le password passe en binaire et en clair, mais est-ce vraiment un hack quand c'est écrit directement dans la notice constructeur et que c'est le fonctionnement normal de la puce d'envoyer les informations en clair ? Sur la capture ci-contre on a un exemple de signal capturé et son décodage : on retrouve notre mot de passe de tout à l'heure 111100(...) ! Il est maintenant possible de dupliquer et/ou de modifier notre propre clé ainsi que la zone password sans la connaître préalablement, à condition que l'on possède une machine qui la connaisse et que pendant la communication avec notre clé, nous sniffions les trames qui passent [Note du rédacteur en chef : « *Bon, je le bois quand mon café moi ?*»].



08 UN TEST FINAL SUR MACHINE RÉELLE ?

Il est bien sûr évident que l'on ne viendra pas avec notre scanner de fréquence ou autre système d'enregistrement réglés sur une fréquence de 125khz, avec une clé modifiée avec une spire d'espionnage supplémentaire et que l'on ne lancera jamais l'enregistrement des trames qui passent pendant qu'une innocente pièce de 30 centimes chargera notre innocente «clé café»... Et non, on ne se permettra pas de modifier la somme présente dans la clé par une autre somme par exemple 59.99€... Bien évidemment, on ne se permettra pas de faire ça, car les essais avec des clés invalides sont comptabilisés et loggués et vous vous feriez vite fait blacklister. De plus, lorsque la balance cash IN/OUT des clés de l'entreprise deviendra négative, une alerte sera levée sur le logiciel de gestion de l'exploitant, et on retrouvera l'identifiant unique qui a servi à voler de l'argent... Ne jouez pas au petit voleur ça finira forcement par se savoir, ce n'est qu'une question de temps...

LE PHISHING : ÉTUDE DE CAS

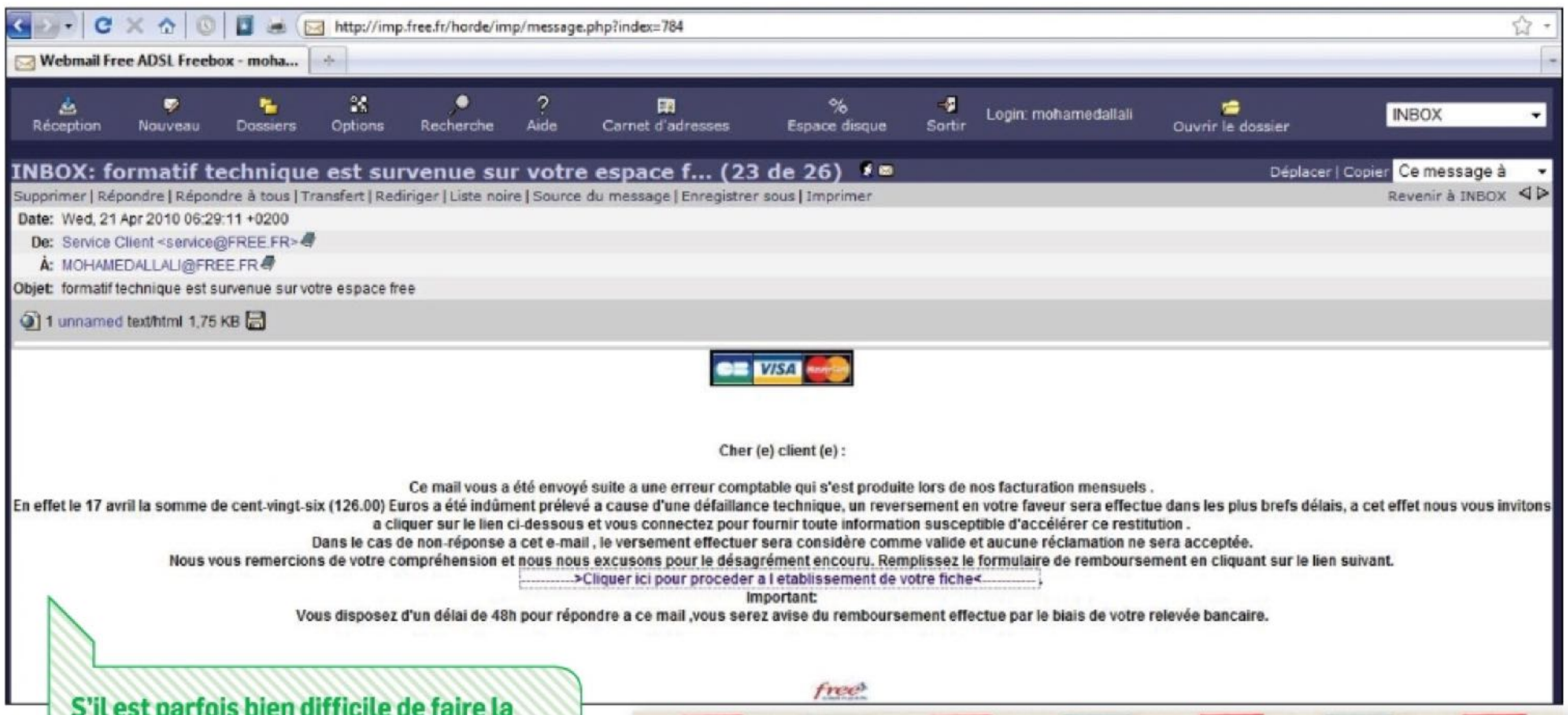
Le phishing est une technique très prisée des pirates puisqu'elle est souvent sans risque pour eux. Seule trace de leur méfait, une page Internet qui peut très bien disparaître ou être hébergée à l'étranger. Le bénéfice est immédiat et assuré d'autant que les techniques ont tellement évolué qu'il est parfois bien difficile de faire la différence entre une page légitime et une page frauduleuse. Selon le Microsoft Computing Safety Index, l'impact mondial annuel du phishing atteint 5 milliards de dollars...

Merci à la team ***Bl@ckBird*** *pour la partie technique de cet article*

LEXIQUE

***PHISHING :**
Le phishing ou « hameçonnage », est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes en se servant d'un e-mail ou d'un lien censé émaner d'une source de confiance (CAF, FAI, banque, etc.)

La technique du phishing est une technique d'«ingénierie sociale», c'est-à-dire consistant à exploiter non pas une faille informatique, mais la «faille humaine» en dupant les internautes par le biais d'un lien (la plupart du temps via un courrier électronique) semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce. Le message les invite à se connecter en ligne par le biais d'un lien hypertexte et de mettre à jour des informations les concernant dans un formulaire d'une page Web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, un problème, un gain ou un remboursement. Pour ce faire nous utiliserons différents outils comme SPF (SpeedPhish Framework), un outil python conçu pour permettre la reconnaissance rapide et le déploiement d'exercices simples d'hameçonnage d'ingénierie sociale. Comme il s'agit de s'amuser et de comprendre les mécanismes de cette technique de pirate, nous éluderons certains aspects. Il s'agit d'une démonstration, nous vous déconseillons formellement de l'utiliser pour piéger des tiers : le script n'est pas fait pour cela et vous vous feriez forcement attraper. Il s'agit ici de tester la crédulité des gens pour une expérience sociale par exemple.



S'il est parfois bien difficile de faire la différence entre une page légitime et sa copie frauduleuse, il ne faut pas être naïf. Dans le doute, connectez-vous au site en suivant la voie normale et pas en cliquant sur un lien. Attention à ces types de messages...

Message de votre CAF :
vous êtes éligible à une aide
X d'une somme de 215 €,
Connectez-vous depuis ce lien

ALLOCATIONS FAMILIALES

BNP PARIBAS

La BNP vous invite à vous connecter d'urgence à votre compte en cliquant sur ce lien pour récupérer la somme de 365,36 € frauduleusement prélevée le 15 juillet dernier».

PayPal

Votre compte PayPal a été désactivé ! Connectez-vous sous 3 jours via ce lien pour ne pas perdre votre argent

LA FAILLE «PUNYCODE» : COMMENT SE PROTÉGER ?

Le phishing connaît une nouvelle étape dans la tromperie. Alors que les pirates essayent de copier au plus près les adresses de sites ou de les rendre vraisemblables, certains sont encore plus malins puisqu'ils utilisent la prise en compte des caractères spéciaux dans les barres d'adresse des navigateurs. En effet il était impossible de mettre des caractères accentués et encore moins des caractères issus d'autres alphabets que le latin, mais c'est terminé avec le «punycode», un nouveau codage. Or quoi de plus ressemblant à un «a» qu'un autre «a» ? La différence c'est que malgré leur ressemblance, la première lettre est un «a» latin (code ASCII : U+0061) tandis que la deuxième est un a cyrillique utilisé dans la langue russe ou ukrainienne (ASCII : U+0430). Sur Firefox il existe une solution. Dans le champ d'URL, tapez **about:config** puis cherchez la clé **network.IDN_show_punycode** et changez cette dernière en **true** avec un double clic. Les noms de domaines s'afficheront «normalement».

PAS À PAS

Le phishing en réseau local

CE QU'IL VOUS FAUT

SPEED PHISHING FRAMEWORK

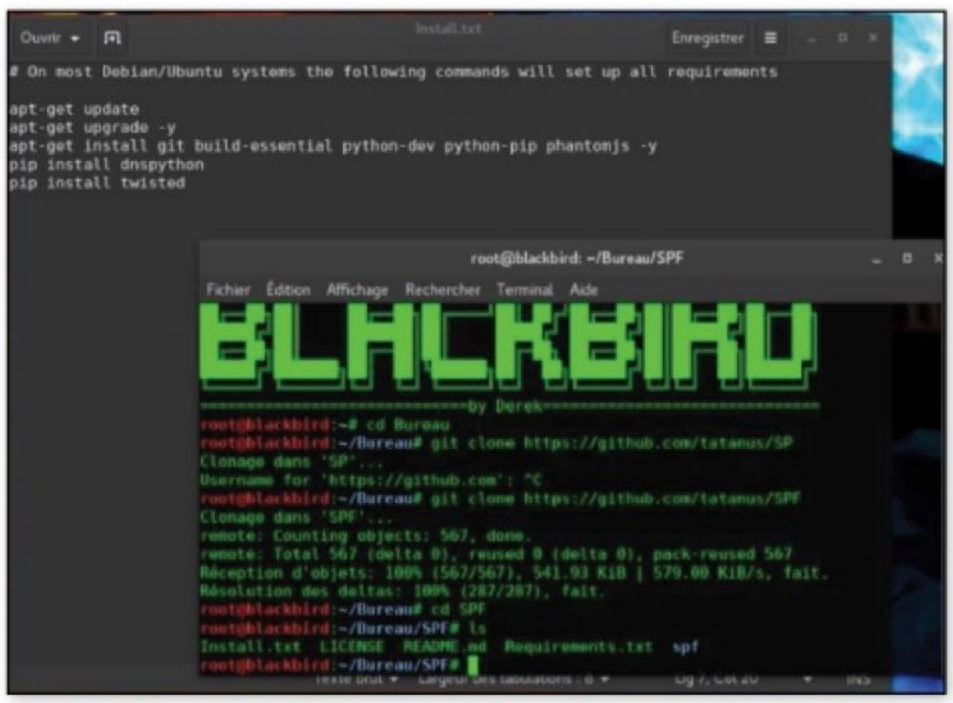
OÙ LE TROUVER ? :
https://github.com/tatanus/SPF.git

DIFFICULTÉ :

01 INSTALLATION

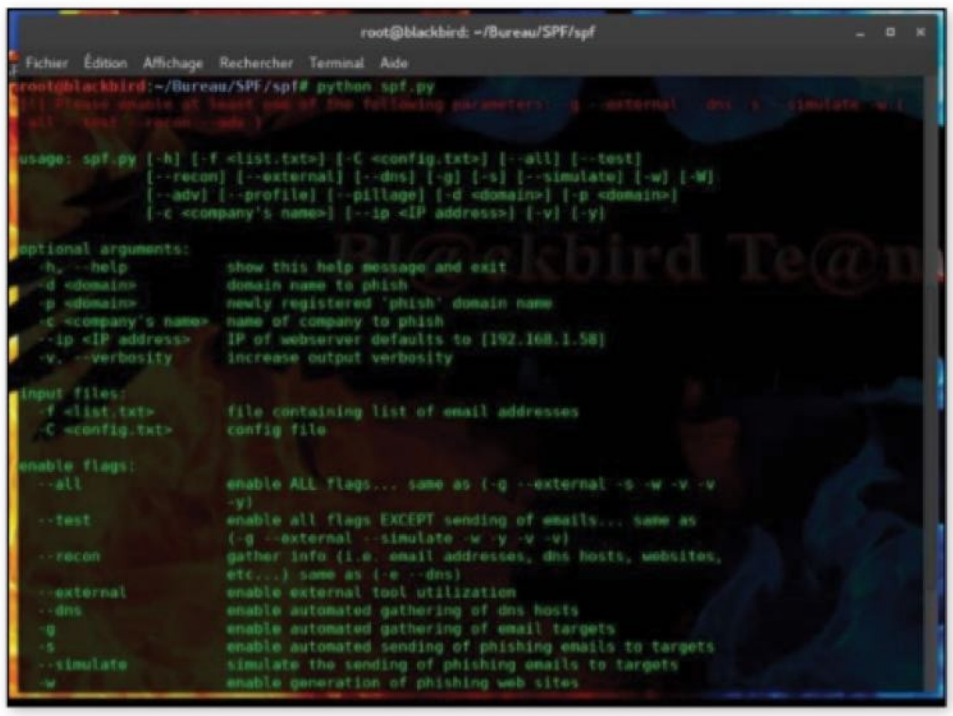
Commençons par installer le script SPF (Speed Phishing Framework) qui nous servira pour cette petite expérience. Pointez vers le bureau avec **cd** (pour que le dossier soit créé sur le bureau) et faites:
git clone https://github.com/tatanus/SPF.git

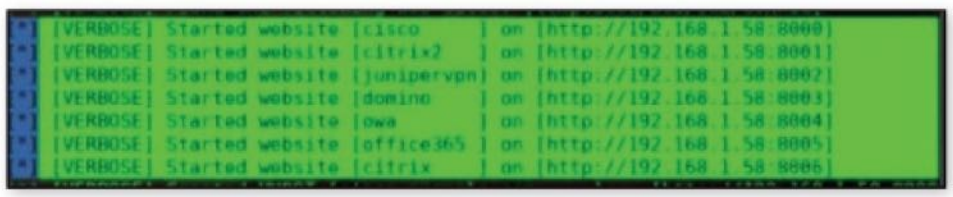
Avec le terminal, dirigez-vous dans le dossier SPF, ouvrez le fichier **install.txt** et effectuez les installations requises:
pip install -r Requirements.txt



02 PREMIER ESSAI

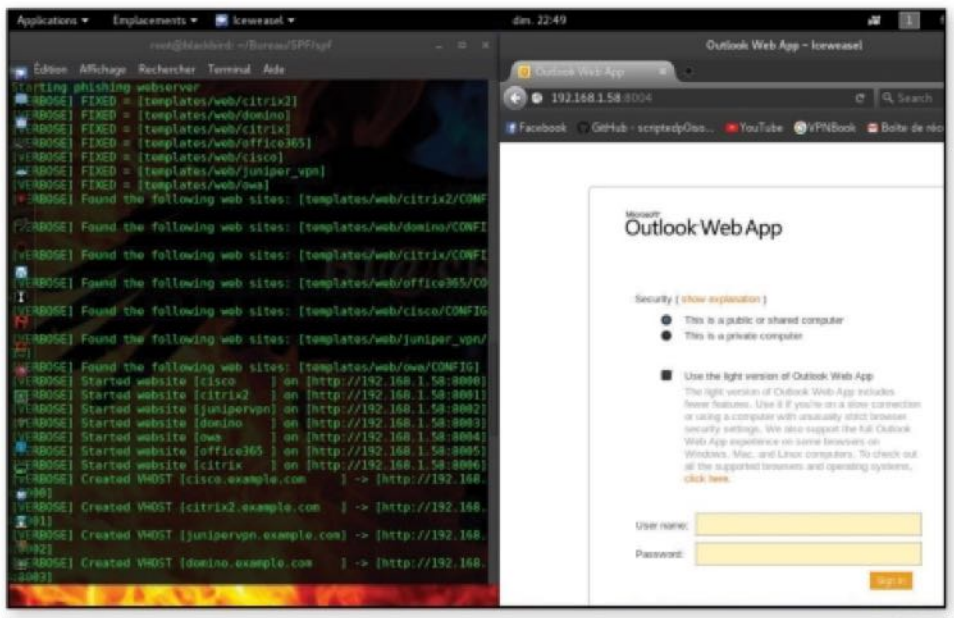
Dirigez-vous maintenant dans le dossier **spf** pour pouvoir accéder au script **spf.py**. SPF comporte déjà des clones de sites (Cisco, Office363, etc.)
Tapez la commande suivante:
python spf.py (-d https://www.facebook.com - -test) ou **–all**, pour débuter le phishing webserver

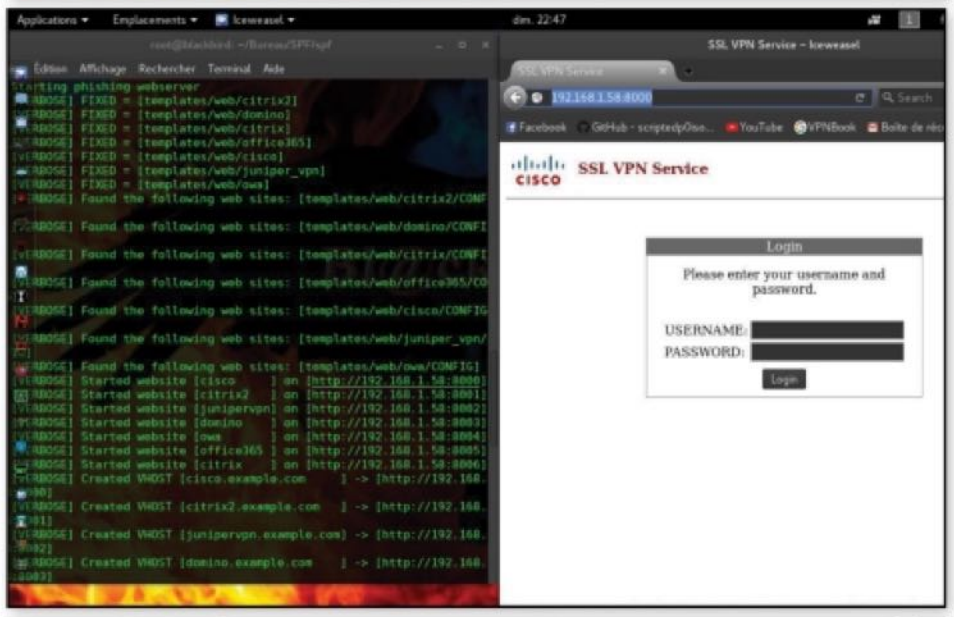


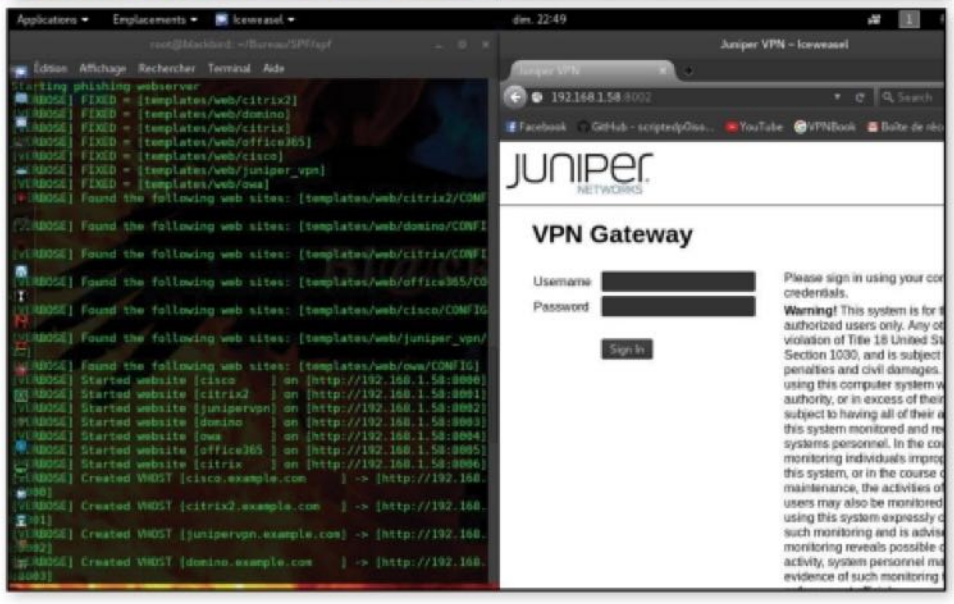


Les liens sont sous la forme http://192.168.1.58:8080. Il vous suffit d'envoyer ce lien à une personne sur le même réseau que vous.

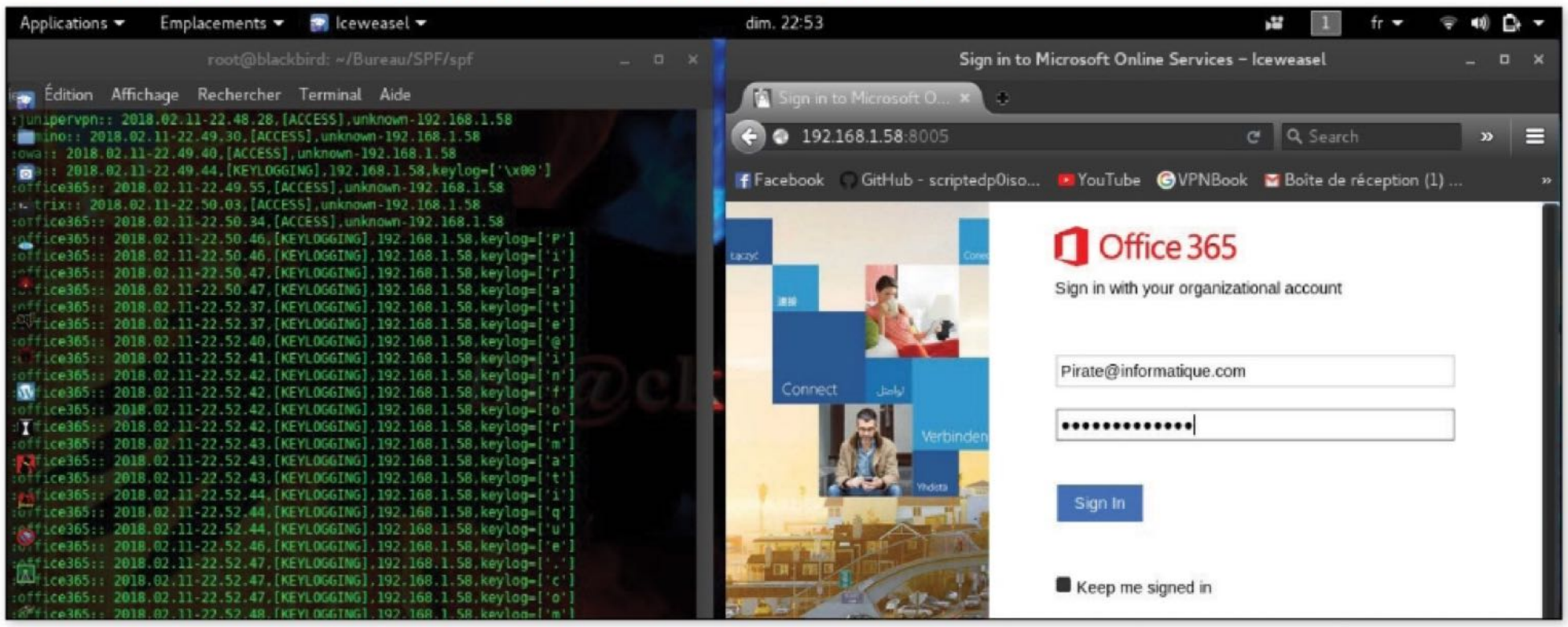
03 TOUR D'HORIZON DES PAGES WEB FACTICES







04 UN SCRIPT QUI FAIT AUSSI KEYLOGGER



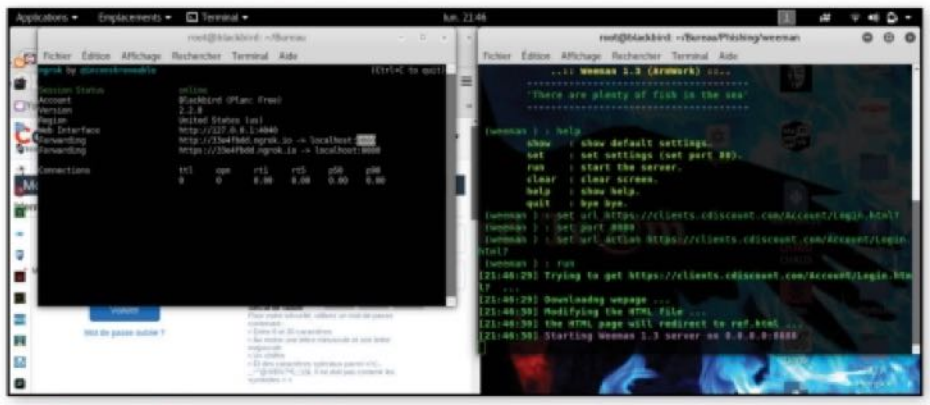
05 TENTATIVE EN DEHORS DU RÉSEAU LOCAL

Pour exploiter cette démonstration en dehors de votre réseau local, il vous faudra ngrok (https://ngrok.com) et le script weeman (https://github.com/evait-security/weeman)
En premier lieu, ouvrons ngrok:
./ngrok http:8080

Ensuite, ouvrons le script weeman que vous aurez installé sur votre bureau.

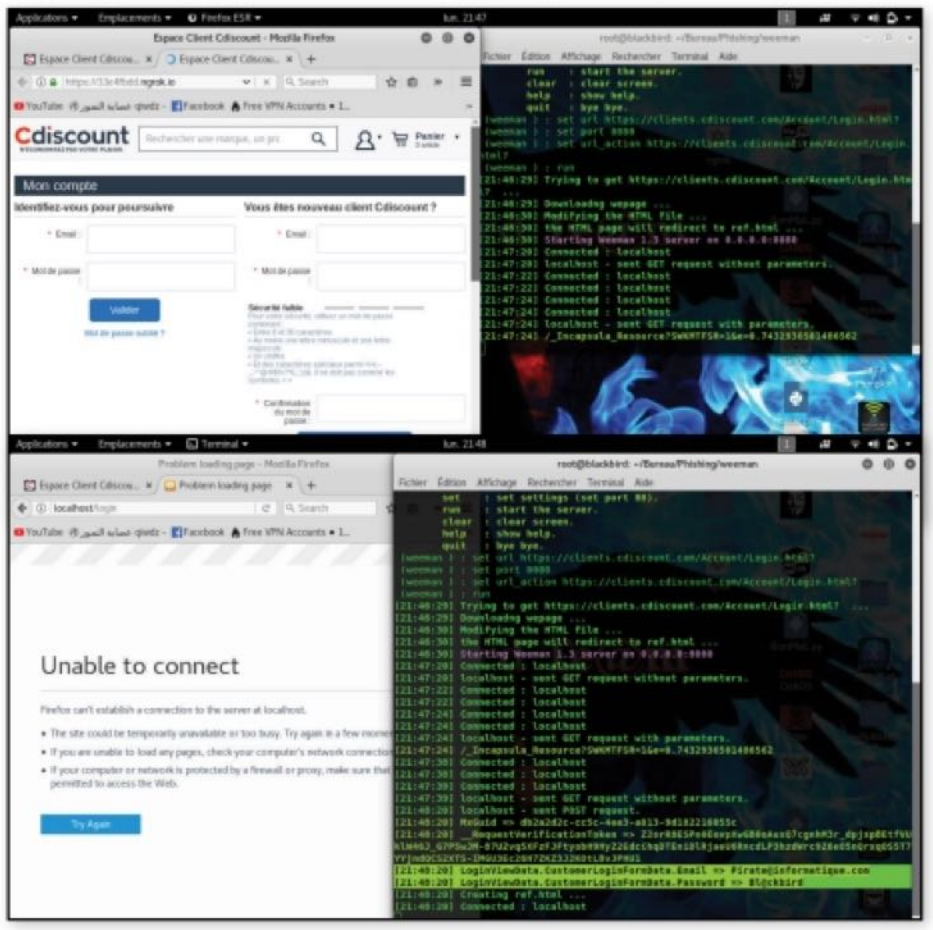
06 NOTRE FAUX SITE

Imaginons que nous voulions faire un clone du site de Cdiscount. Il suffit de copier l'URL du site et de le coller sur weeman. Le port sera celui en écoute sur ngrok (ici 8080).
Pour les commandes:
Set url https://.....
Set port 8080
Set action_url https://.....



07 RÉCUPÉRATION DES IDENTIFIANTS

Ensuite, sur le terminal de ngrok copions le lien https://33e4fbdd... que nous collerons sur un navigateur pour voir le clone du site. Nous pouvons voir que le clone est plutôt réaliste, essayons de saisir un e-mail et mot de passe... Après avoir validé le script en cliquant, il récupère les informations: identifiant et mot de passe en clair. Nous avons pris en exemple le site de Cdiscount, mais d'autres sites comme SFR, Amazon, PayPal peuvent servir de clone pour le phishing.

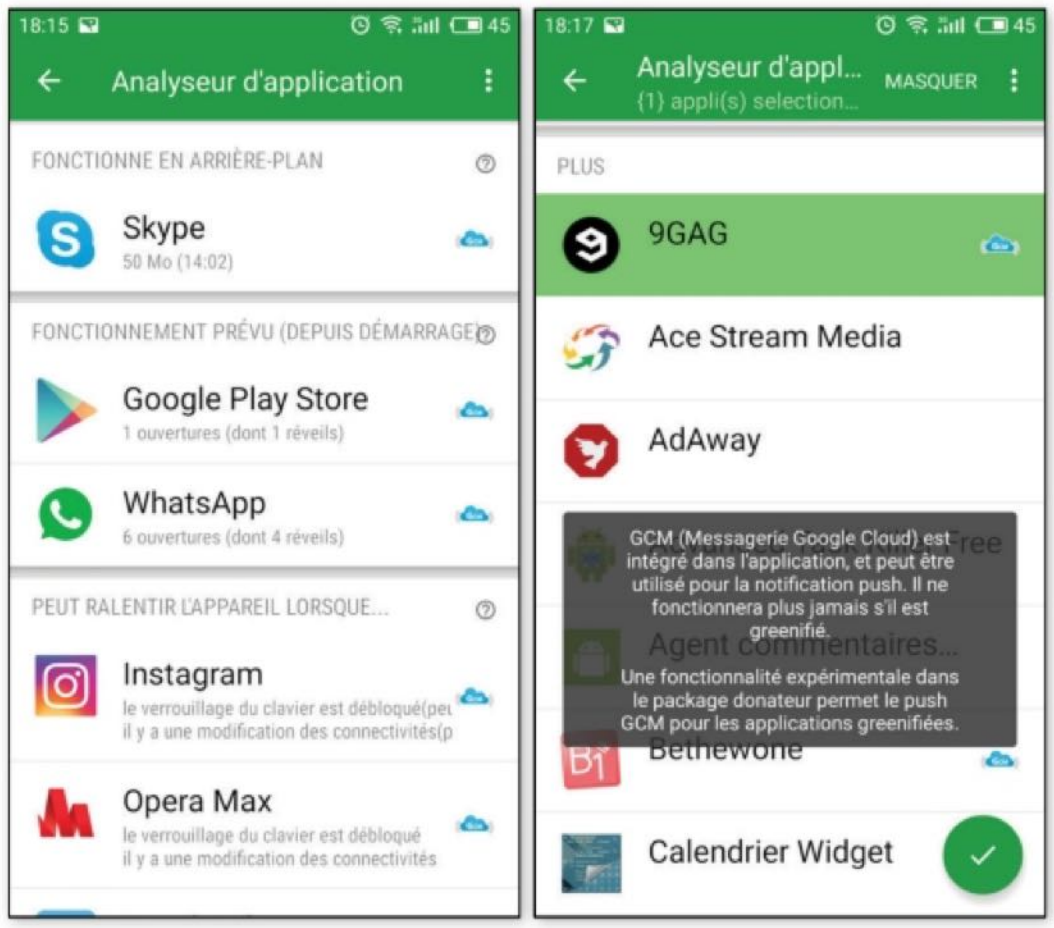


#1 Faites hiberner vos applications

AVEC GREENIFY

Si vous êtes sous Android, vous savez que la batterie fond comme neige au soleil lorsque les applications se mettent à fonctionner sans votre consentement. Greenify permet de les «figer» pour économiser de la batterie et gagner en puissance... L'appli fonctionne mieux et offre plus de latitude sur un appareil rooté mais ce n'est pas obligatoire. En mode root par exemple, vous pourrez utiliser une «hibernation intelligente» : en bref, l'appli dormira jusqu'à ce que vous la réveillez. Il faudra pour cela autoriser l'appli Greenify à avoir accès à l'état de fonctionnement des autres applis. Faites juste **Accorder l'autorisation** et activez Greenify. Ensuite, rien de plus simple : sélectionnez les applications qui vous ennuient (les bloatwares fournis de base avec votre téléphone, les applications que vous ne pouvez pas désinstaller, etc.) et ajoutez-les à votre liste d'hibernation. Une fois hibernées, vos applications n'iront plus chercher de mises à jour ou s'allumer de manière intempestive pour aller fureter sur le réseau. Vous économiser votre batterie et le processeur sera plus réactif puisqu'il ne sera pas embêté avec des processus qui se lancent constamment.

Lien : **https://play.google.com/store/apps/details?id=com.oasisfeng.greenify**

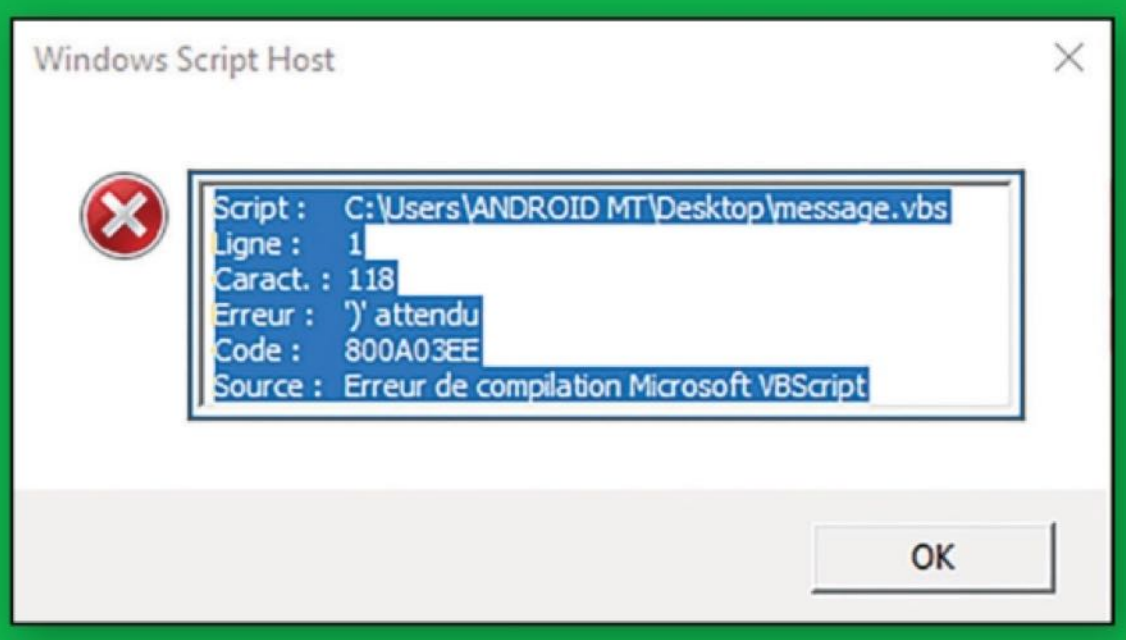


#2 Copier un texte non sélectionnable

AVEC TEXTIFY

Si vous tombez sur un texte (message d'erreur Windows par exemple) qui n'est pas sélectionnable, mais que vous avez besoin de copier, Textify outrepasse cette restriction. Dans les options du logiciel, sélectionnez la combinaison que vous souhaitez : ici, nous avons choisi d'appuyer en même temps sur le bouton droit de la souris et de maintenir la touche **Maj**. Utilisez cette combinaison sur le texte et il deviendra sélectionnable. Cela fonctionne avec tout texte non sélectionnable dans Windows.

Lien : **http://rammichael.com/textify**



#3 Comment placer Windows sur une clé USB

AVEC WINTOBOOTIC

Si notre article sur WinToFlash ne vous a pas convaincu, sachez qu'il existe de nombreux autres logiciels permettant de placer une installation de Windows sur une clé USB : Rufus, UNETBootin, Yumi, etc. Le nouvel arrivé dans cette catégorie nous vient d'Ukraine et se nomme WiNToBootic. Ce dernier facilite la création d'une clé USB ou d'un DVD bootable pour vos systèmes d'exploitation Windows 7, 8 et 10. Même s'il se concentre uniquement sur les systèmes Microsoft, il est très rapide et propose plusieurs fonctionnalités sympas.

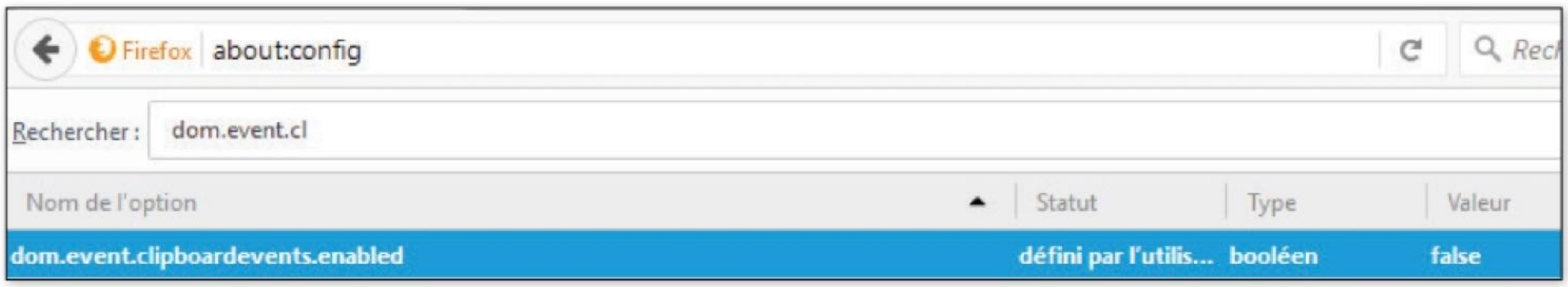
Lien : **http://wintobootic.findmysoft.com**

#4 Coller du texte sur les sites qui le refusent

AVEC FIREFOX

Sur certains sites, il est impossible de coller du texte dans un champ de saisie, il faut obligatoirement taper au clavier. Mais avec Firefox, une petite astuce permet de contourner ce blocage. Ouvrez une fenêtre ou un onglet vierge et tapez **about:config**. Cochez le **Je prends le risque**. Tapez ensuite **dom.event.cl** dans le champ **Rechercher**. Double-cliquez sur **dom.event.clipboardevents.enabled** pour que sa valeur passe à **False**. Fermez l'onglet, c'est effectif immédiatement.

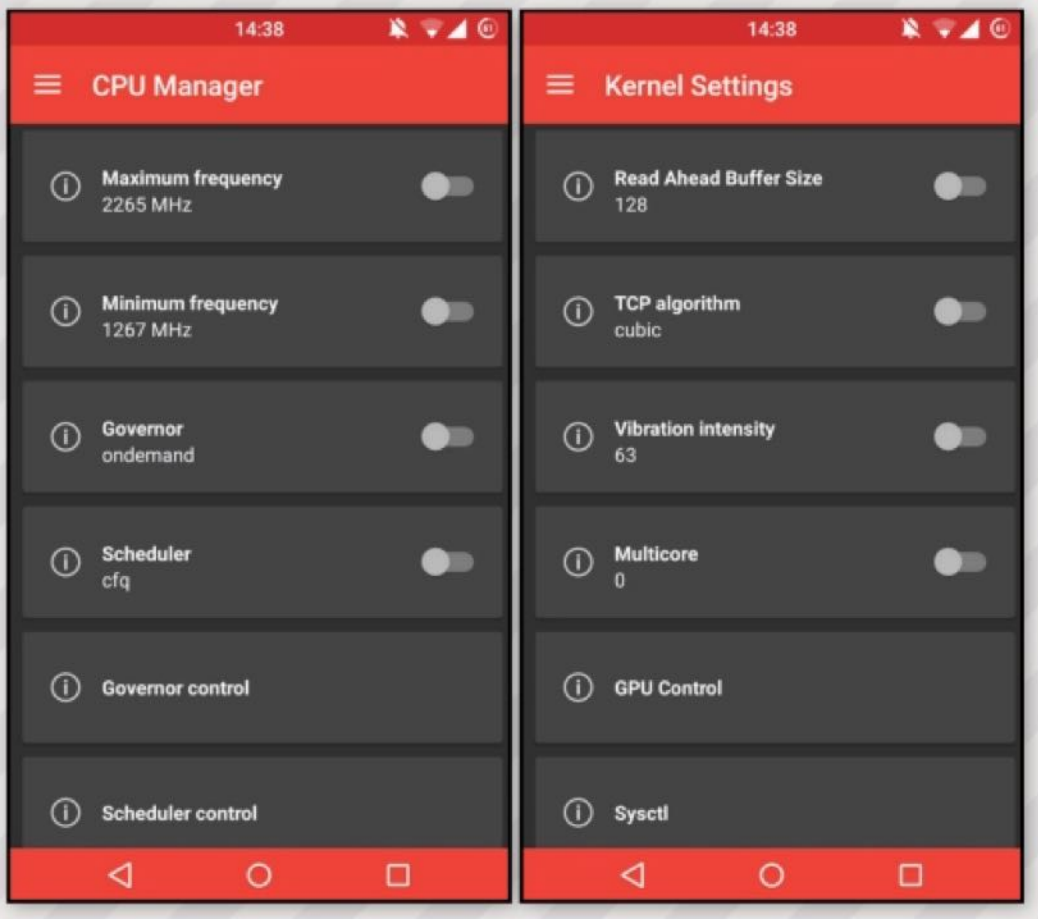
Lien : **www.mozilla.org/fr/firefox**



#5 Un appareil Android sous contrôle total

AVEC KERNEL MANAGER

Vous êtes l'heureux possesseur d'un mobile rooté et vous cherchez une boite à outils pour exploiter tout le potentiel de votre appareil ? L'application Kernel Manager est la réponse à votre problème.



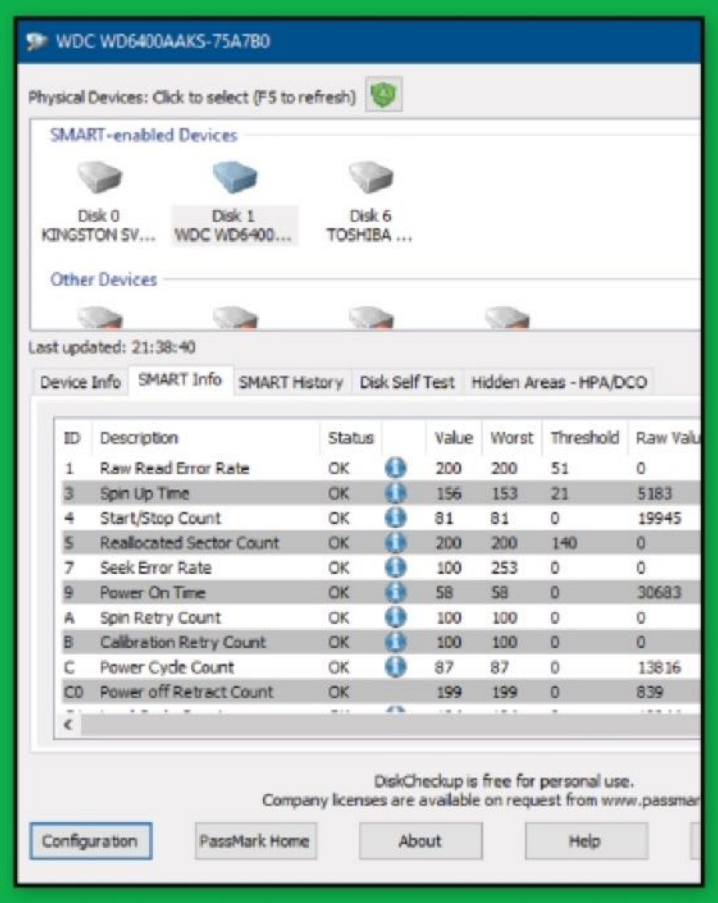
Le nombre d'options de paramétrage est ahurissant : changer la fréquence du CPU, mettre l'appareil en sous-tension ou en surtension, modifier l'intensité du vibreur, gérer le niveau sonore du casque et du haut-parleur du téléphone, etc. Fonction intéressante, la possibilité de créer des profils d'utilisateurs, pour adapter tous ses paramètres selon l'usage (quotidien, économie d'énergie, performance, etc.) Une appli très complète, qui demande néanmoins des connaissances techniques sur Android.

Lien : **https://play.google.com/store/apps/details?id=com.simonedev.kernelm**

#6 Vos disques sous surveillance

AVEC DISKCHECKUP

DiskCheckup effectue des tests sur votre disque dur et surveille en temps réel une multitude de paramètres : temps d'accès, latence, débits en lecture et écriture, taux d'erreurs, température, etc.



En cas de dépassement de certains seuils critiques, il peut afficher une fenêtre d'avertissement, ou bien envoyer un mail à l'adresse de votre choix : une disposition bien pratique pour contrôler h24 les disques d'un serveur.

Lien : **https://tinyurl.com/q33a98j**

KODI :

CENTRALISEZ VOS FICHIERS MULTIMÉDIAS

Le logiciel Kodi est un outil remarquable lorsqu'il s'agit de récupérer votre petit monde numérique depuis le réseau, un disque dur ou Internet. Il est aussi multiplate-forme : vous pouvez très bien l'installer sur un vieux PC, un Mac ou un Raspberry Pi. Il existe aussi des versions Android préinstallées sur des box multimédias, très à la mode en ce moment...

Kodi a commencé sa carrière en 2003 sous le nom de XBMC. Il s'agissait en fait d'un Media Center pirate sur les premières Xbox modifiées. Le logiciel a fait du chemin puisqu'il a successivement séduit les utilisateurs de Windows, Linux, Android, Mac OS et iOS. Le prix plancher et la compacité du Raspberry Pi ont aussi suscité l'intérêt des développeurs pour ce nano-ordinateur et c'est tout naturellement qu'on trouve des versions compatibles. À chaque fois la recette est la même : le but est de réunir tous vos fichiers multimédias sur une même interface pour les retrouver facilement et ne pas avoir à lancer un logiciel pour vos MP3, un autre pour vos films, un autre pour télécharger, etc. Une fois installé sur votre PC, il faudra passer quelques

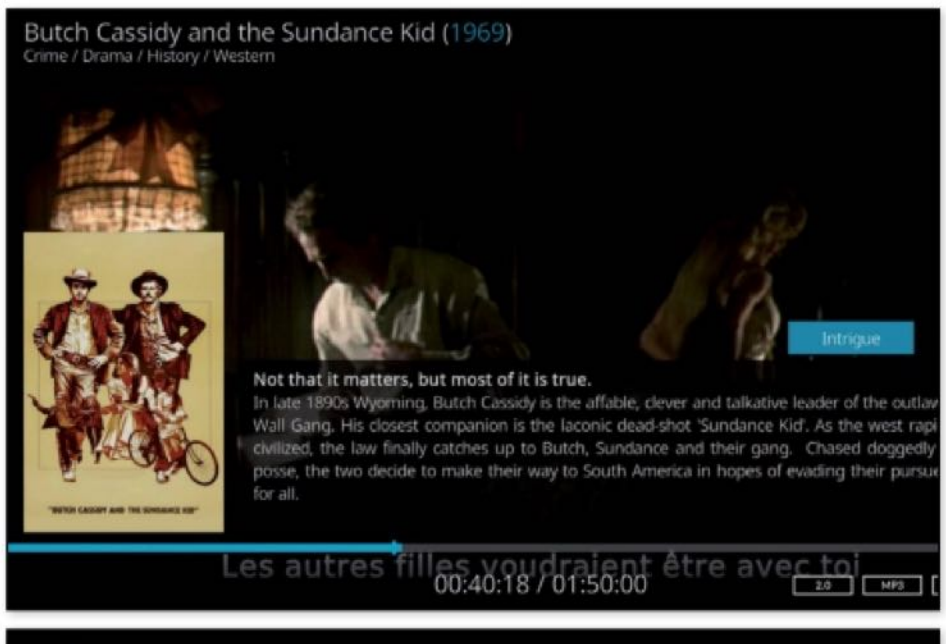
LEXIQUE

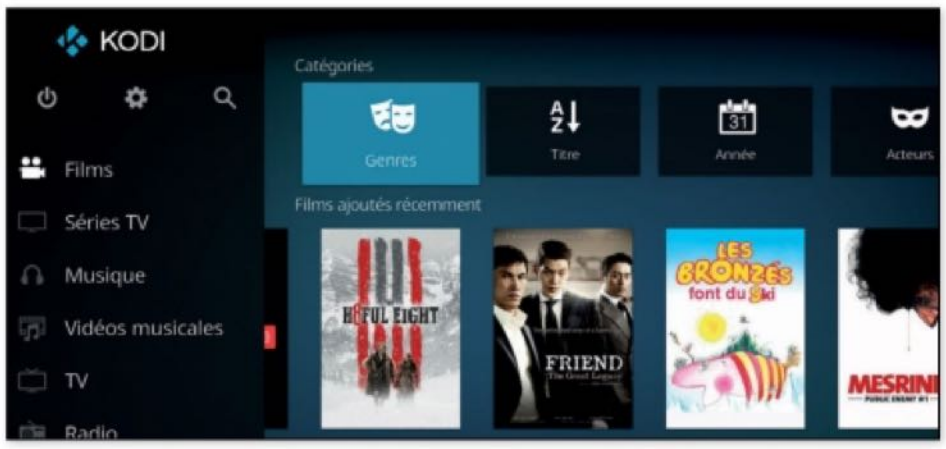
***MEDIA CENTER :**
Media Center peut désigner un disque dur multimédia relié à une TV ou un Home Cinema mais il peut aussi désigner la partie logicielle de ces derniers. Kodi est un programme qui peut se greffer sur presque n'importe quel système pour en faire une interface de lecture conviviale.

minutes à le paramétrer pour lui dire où aller chercher tel ou tel fichier, choisir son thème, trouver l'accès aux autres machines, etc. La prise en charge du réseau est d'ailleurs un gros plus puisque vous pouvez très bien «aller chercher» vos photos, musiques et films sur un autre PC faisant office de serveur, un NAS ou même un appareil mobile. Les protocoles compatibles sont légion (UPnP, SMB, NFS, etc.) et l'interface n'a rien de bien compliquée.

UNE INTERFACE PERSONNALISABLE

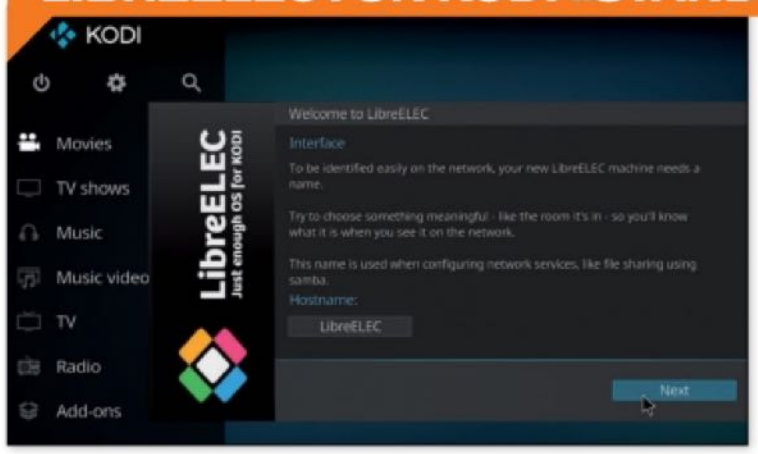
Kodi se révèle très impressionnant dans votre salon. En effet, si vous avez un vieil ordinateur, il est très facile de se confectionner un Media Center digne de ce nom puisqu'il est même possible d'ajouter une télécommande (même si nous vous conseillons ces minis clavier/trackball Bluetooth). Mais comme avoir une vieille tour qui fait du bruit sous la TV n'est pas du goût de tout le monde, des fabricants se sont mis à proposer des «box» multimédias sous Android ou Android TV qui proposent Kodi : compact, sans ventilateur et esthétiquement réussi, c'est quand même bien mieux (voir notre encadré) ! Le logiciel supporte presque tous les formats et extensions de fichiers multimédias même les plus récents. Il intègre en plus des fonctionnalités comme la compatibilité avec les formats les plus courants de playlist, des diaporamas, la possibilité de streamer ou d'écouter des radios Internet comme SHOUTcast et Last.fm. La communauté est tellement vivace que de nombreux plugins sont développés pour permettre d'enrichir votre interface. Il est, par exemple, possible d'avoir des bulletins météo, de récupérer des sous-titres directement depuis l'interface ou d'avoir accès à des bases de données pour récupérer des informations sur vos albums ou vos films. Il est même possible de télécharger en utilisant Torrent, de regarder ses mails ou d'avoir accès à sa page Facebook. Si vous utilisez votre PC pour vos loisirs numériques, vous allez vite délaisser Windows pour ne plus jamais sortir de ce Media Center !





Interface, confort d'utilisation, nombres de plugins : Kodi est de loin le meilleur media center grâce à sa communauté très vivace.

LIBREELEC : UN KODI «STAND ALONE» SOUS RASPBERRY PI



Le Raspberry Pi est une très bonne machine pour se confectionner un media center à bas coût. Si vous avez le système Raspbian, vous pouvez très facilement l'installer. De même Kodi est présent dans la plate-forme de retrogaming Recalbox, mais il existe aussi des distributions spécialisées avec uniquement Kodi. Parmi celles-là, nous vous conseillons LibreELEC. Le but d'avoir un système dédié à Kodi est d'économiser les ressources du Raspberry Pi. Les résultats sont surprenants et l'interface est la même: vous pouvez donc suivre sans problème notre pas-à-pas !
Lien : https://libreelec.tv

PAS À PAS

Premier pas avec Kodi v17

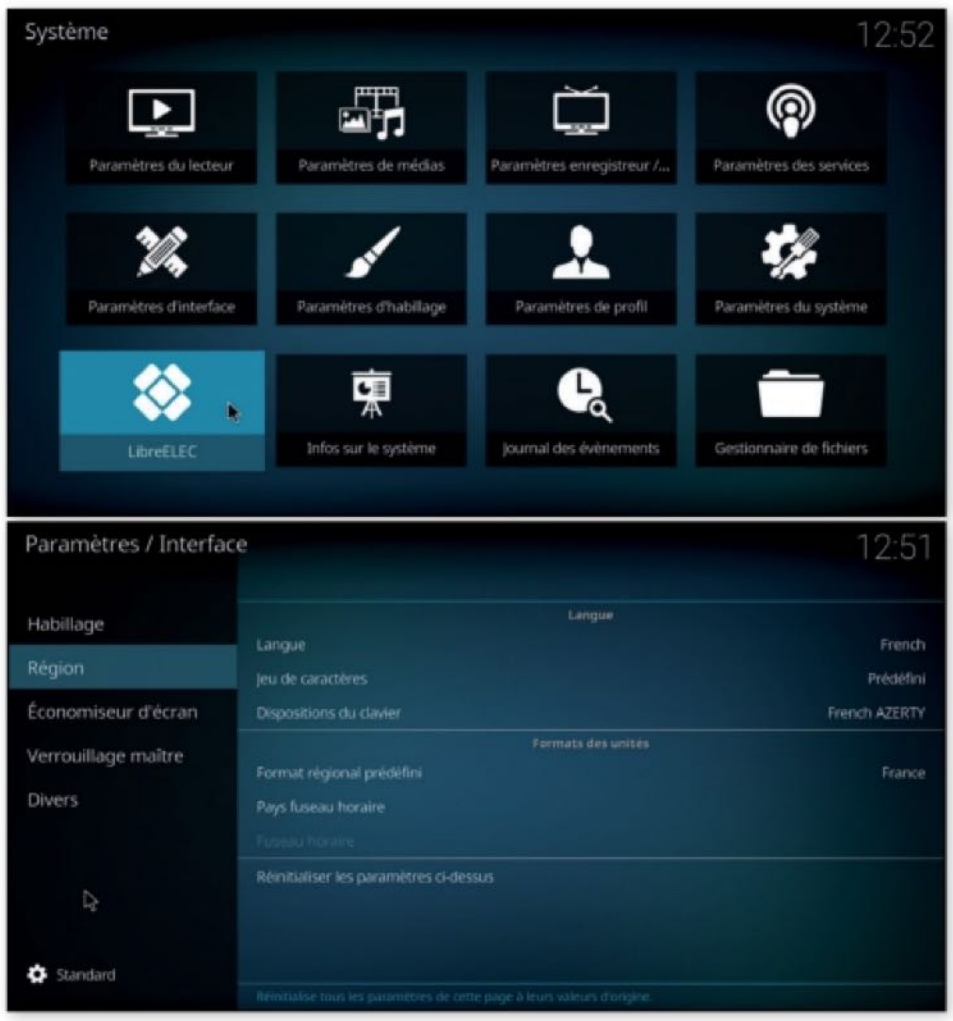
CE QU'IL VOUS FAUT

KODI 17 (KRYPTON)

OÙ LE TROUVER ? : **http://kodi.tv**

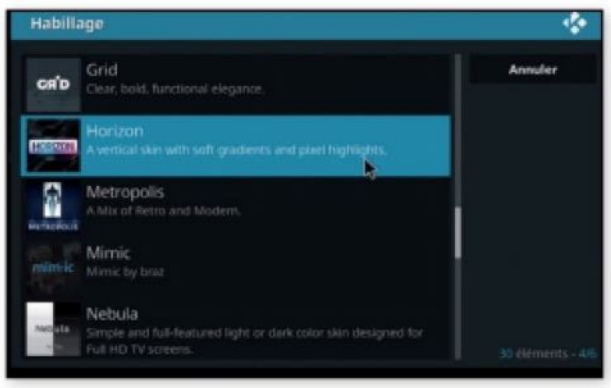
DIFFICULTÉ :

01 L'INSTALLATION



Nous n'allons pas expliquer la procédure d'installation puisque pour chaque machine c'est différent. Si vous avez une box Android, installez l'appli depuis le Google Play Store, pour le Raspberry Pi, il faudra flasher une carte micro SD avec le fichier IMG de LibeELEC depuis le logiciel Etcher et pour Windows, il suffit d'installer le fichier EXE et d'autoriser Kodi à passer à travers votre pare-feu. Notez que vous n'avez pas besoin d'installer Kodi sur tous vos appareils : uniquement celui qui est branché au téléviseur... Depuis la fenêtre principale, allez dans l'engrenage en haut à gauche puis **Interface Settings**. Dans l'onglet **Regional**, cherchez le **Français** et profitez-en pour changer l'agencement du clavier.

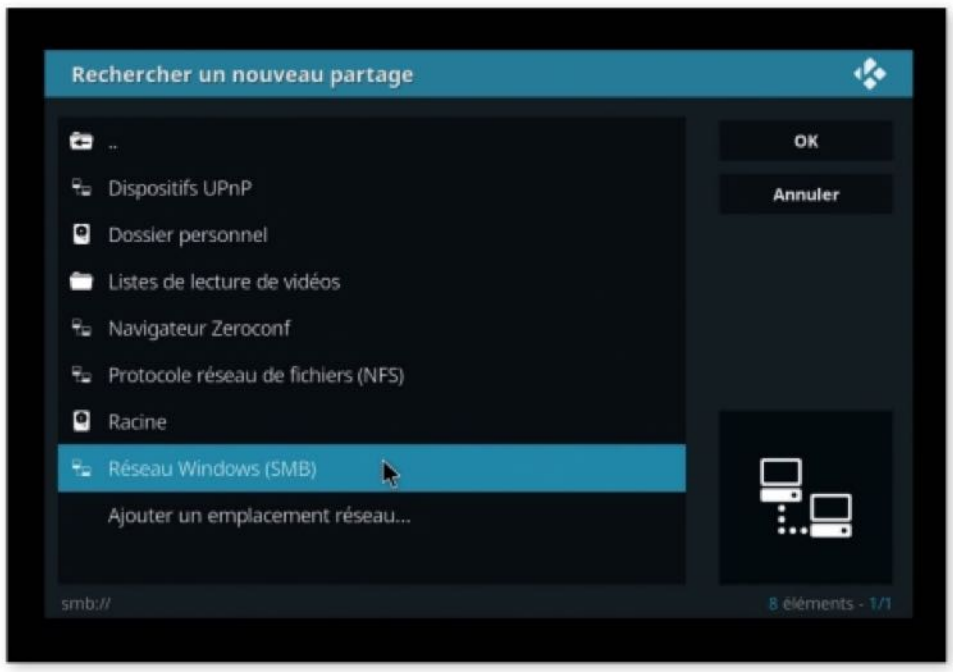
02 VOTRE THÈME



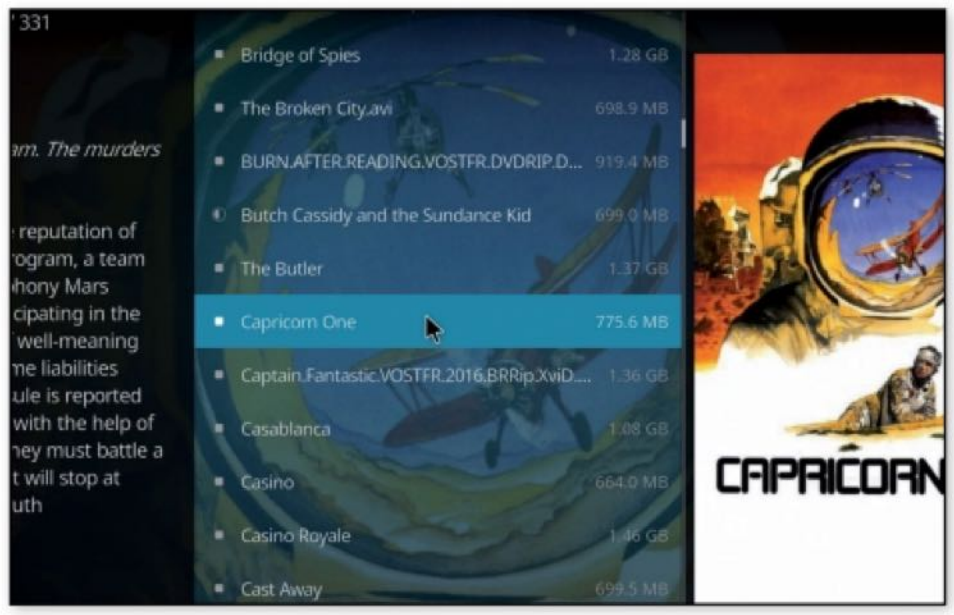
Vous pouvez ensuite aller dans **Habillage** et cliquer sur **En obtenir plus**... pour télécharger d'autres skins. À vous de trouver celui qui vous conviendra le mieux, mais sachez que certains thèmes proposent davantage d'entrées au menu principal comme **Concert, Météo, Série TV**, etc. À moins d'être allergique à celui par défaut, nous vous conseillons de garder ce dernier.

03 TROUVEZ VOS FICHIERS

Pour commencer l'aventure, il va falloir dire au logiciel dans quel(s) dossier(s) aller chercher vos différents répertoires multimédias. Par exemple dans **Films**, cliquez sur **Section « Fichiers »** puis **Fichiers** et **Ajouter une source de vidéos**... Ici, il faudra chercher dans votre disque dur le ou les dossiers où vous avez l'habitude de ranger vos films. Si vous avez plusieurs types de films, rien ne vous empêche de les organiser dans Windows. Il est conseillé de mettre chaque film dans un dossier séparé qui porte son titre, mais ce n'est pas obligé. Si vos contenus sont sur le réseau, nous vous conseillons d'utiliser le protocole Samba en se dirigeant vers l'IP de votre PC ou NAS. Dorénavant, lorsque vous irez dans **Films**, vous aurez tous vos albums et morceaux dans une liste !



04 LES OPTIONS

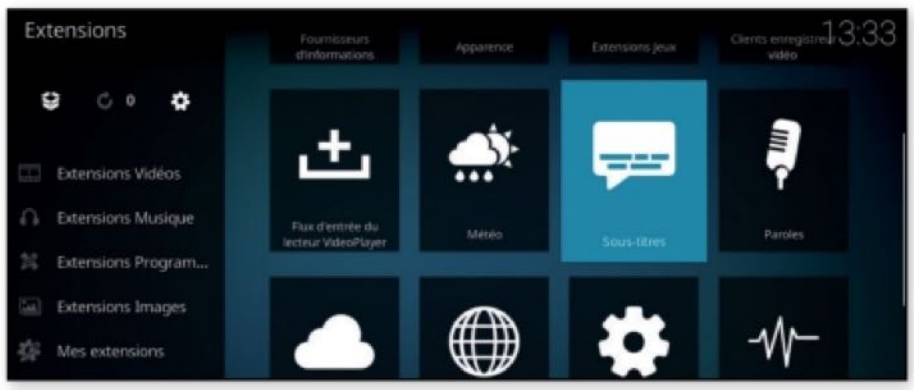


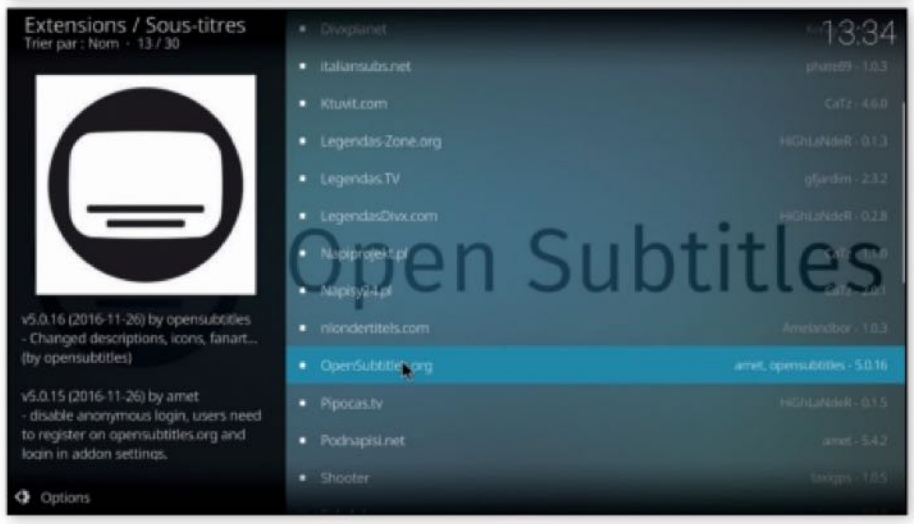
Faites de même dans les autres catégories **Série TV, Images, Musique**. À chaque fois qu'un dossier ou qu'un groupe de dossiers sera analysé par Kodi, vous aurez l'occasion de le « scraper » : depuis une base de données spécialisées (The Movie Database par exemple), vous pourrez télécharger

automatiquement les pochettes de vos albums, les affiches et synopsis de vos films, etc. Vous aurez l'occasion de chercher des films selon la date, le nom des acteurs, etc.

05 AJOUTER DES EXTENSIONS

Pour ajouter une **extension**, il suffit de cliquer dans Extensions puis **Télécharger** choisissez ensuite la rubrique de votre choix. Il en existe des quantités (radio, TV, BitTorrent, chat IRC, Facebook, jeux, etc.), mais celui que vous voudrez installer en premier si vous êtes un fan de VO, ce sont les sous-titres. Nous vous conseillons **OpenSubtitles.org**, très complet : il faudra néanmoins vous créer gratuitement un compte sur le site pour en profiter. Lorsque vous lirez une vidéo, allez dans l'icône correspondante en bas à droite pour télécharger vos sous-titres et les afficher.





XIAOMI MI BOX

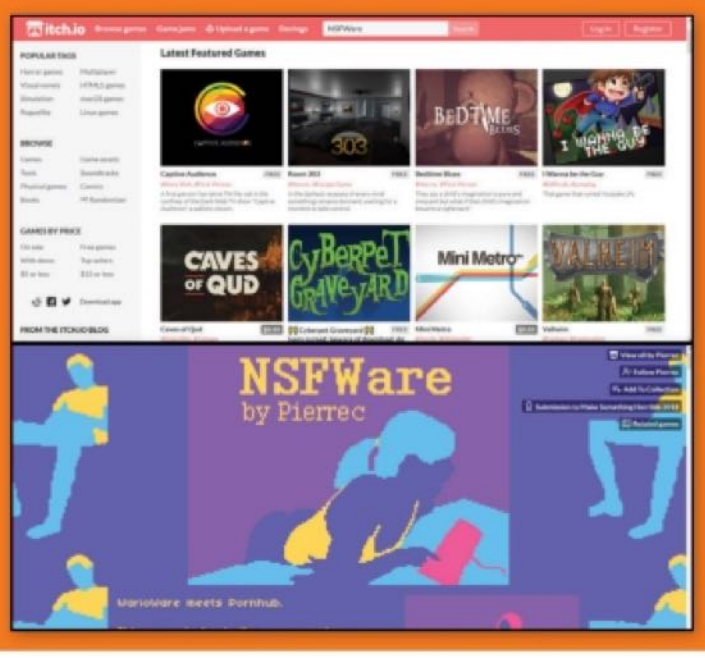
Vous le savez sans doute, mais la marque chinoise Xiaomi a dernièrement débarqué en France. Cette dernière est un peu à part sur ce secteur puisqu'en plus de proposer des smartphones à des prix très attractifs, ils vendent aussi des appareils connectés (aspirateur, montre, etc.) et même des trottinettes électriques ! Mais ce qui nous intéresse ici c'est cette «boîboîte» dont tout le monde parle sur Internet : la fameuse Mi Box. Il s'agit en fait d'un media center à base d'Android TV. Compatible 4K et disposant de nombreuses connectiques, c'est un monstre de puissance qui en fait le media center idéal. Bien sûr, vous aurez aussi à disposition le Google Play Store pour jouer, ajouter des applications (Netflix, Kodi, YouTube, Google Drive, etc.) Et si vous avez une TV 4K alors là, c'est carrément le bonheur.
Pour en savoir plus et profiter d'une promotion : **https://tinyurl.com/yao5dx2t**

#1 Une plate-forme de jeux indés

AVEC ITCH.IO

Itch.io est un site Web qui permet aux développeurs indépendants de jeux vidéo d'héberger, distribuer et vendre leurs jeux. Le site propose plus de 70 000 jeux répartis entre plusieurs systèmes : Android, Windows, Linux, iOS, MacOS ou directement sur son navigateur. La boutique Itch propose une gestionnaire de jeu qui n'est pas obligatoire : un logiciel pour ordinateur de bureau permettant d'installer, mettre à jour, lancer et acheter les jeux. Une sorte de Steam indépendant. Notez que de nombreux jeux sont gratuits, mais que vous êtes invités à faire un don si vous avez aimé une création.

Lien : **https://itch.io**

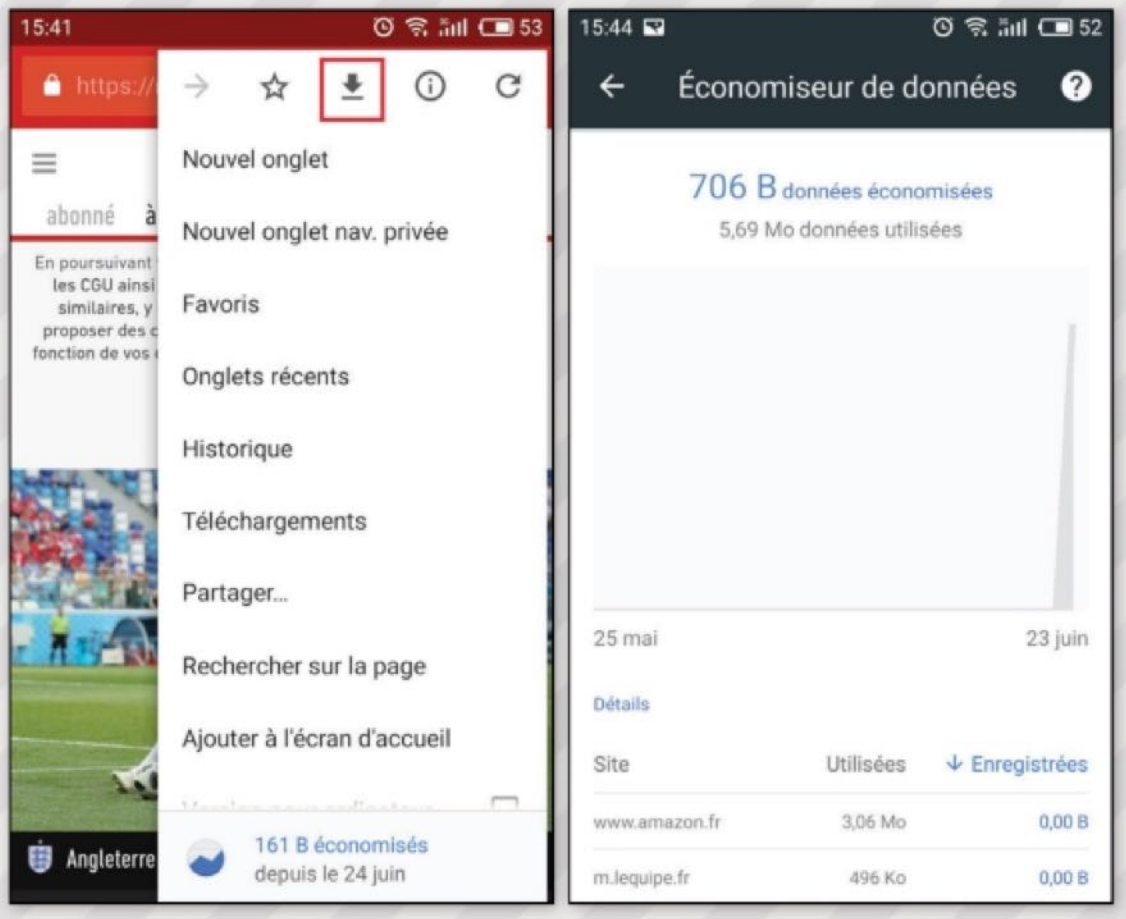


#2 Économisez votre forfait data

AVEC CHROME POUR MOBILE

Vous ne le savez peut-être pas, mais Chrome dispose d'une fonctionnalité «économiseur de données» qui compresse en amont les données des pages consultées pour être rapatriées sur votre mobile en consommant moins de données sur votre forfait «data». Pour en profiter, allez dans les **Paramètres** puis choisissez **Économiseur de données** avant de l'activer. En ce qui concerne la lecture hors ligne, cliquez sur le menu en haut à droite puis sur la petite flèche lorsque vous êtes sur une page Internet. Vous aurez le loisir de la consulter offline plus tard...

Lien : **www.google.com/chrome**



#3 Du son dans toute la maison

AVEC MOODE AUDIO PLAYER

Moode Audio Player, à l'instar de Volumio est une distribution pour Raspberry Pi à destination des audiophiles. Cet OS va transformer votre nano-ordinateur en serveur audio basé sur MPD (Music Player Daemon). Ce dernier permet de diffuser vos morceaux et playlists dans toute la maison et de piloter tout ça avec n'importe quel appareil pourvu d'un client compatible : smartphone, tablette, ordinateur, TV connectée, console de jeu, etc. Moode Audio Player se configure depuis une interface Web, il est compatible avec AirPlay et permet de gérer les DAC (convertisseur numérique-analogique) en USB ou en I2S avec un HAT.

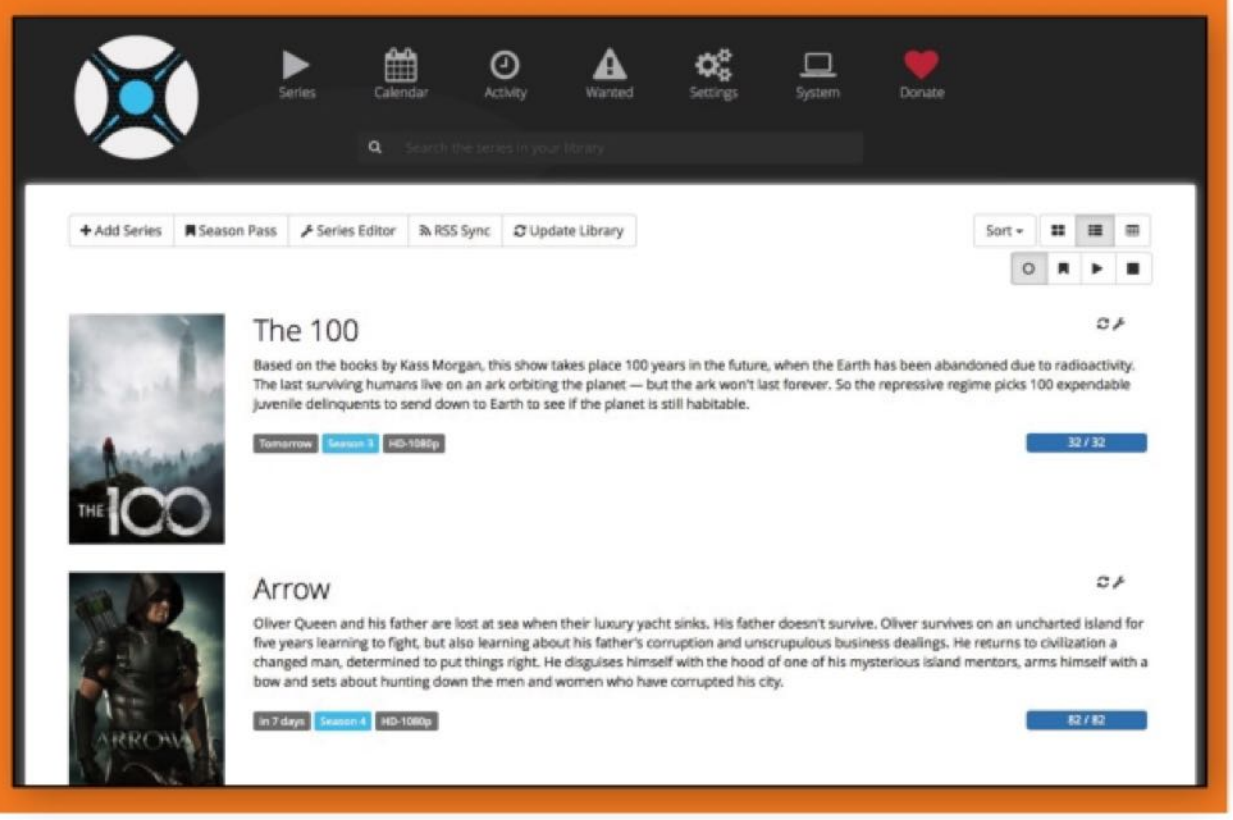
Lien : **http://moodeaudio.org**

#4 Automatisez les téléchargements de vos séries TV

AVEC SONAAR

Sonaar permet de ne plus perdre de temps à chercher le nouvel épisode de chaque série TV que vous suivez. Vous vous réveillez avec les derniers épisodes diffusés la nuit d'avant, prêts à être regardées, dans la qualité que vous souhaitez, et bien rangées là où il faut. À vous de choisir votre plate-forme de prédilection (Windows, OS X, Linux, Raspberry Pi ou encore sur un NAS). Après l'installation vous accédez à une interface Web pour les réglages. Paramétrez vos préférences : emplacement de stockage, client Torrent, qualité du fichier, sous-titres, doublage, etc. Le complice idéal de Kodi (voir page 38)

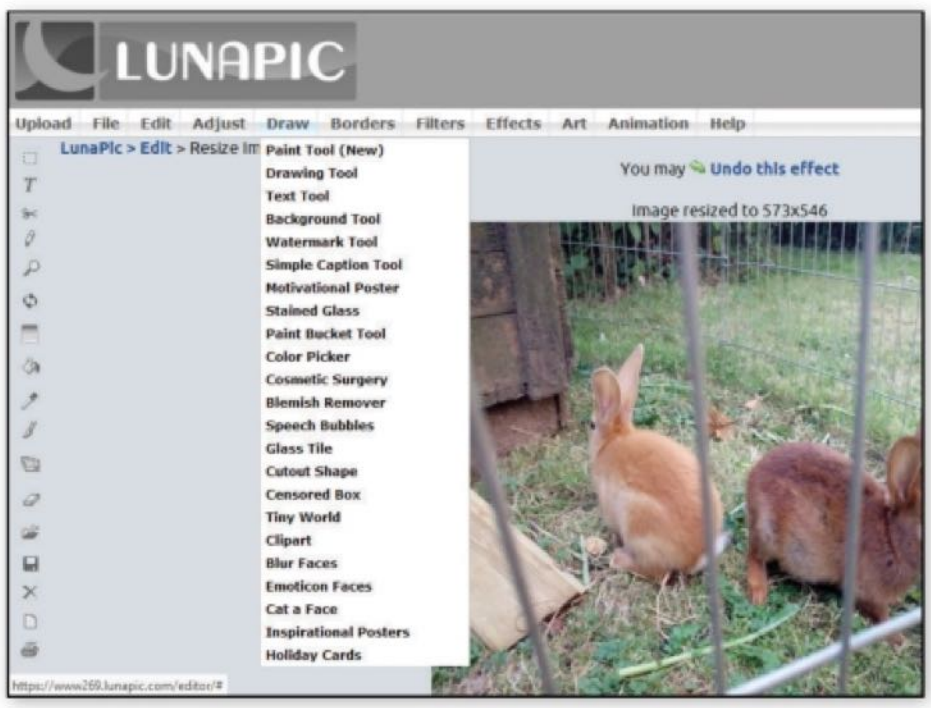
Lien : **https://sonarr.tv**



#5 Tout pour la retouche d'images

AVEC LUNAPIC STAMP

Certaines applications en ligne n'ont pas grand-chose à envier à leurs homologues installés sur PC. C'est le cas de Lunapic, qui offre toutes les fonctions nécessaires pour retoucher vos images (contraste, luminosité, couleurs, recadrage, etc.) et plus de 200 filtres et effets photo. Un petit temps de prise en main sera nécessaire pour exploiter toutes ces possibilités. Attention, le site



est en anglais. Connectez-vous sur le site de Lunapic. Puis cliquez sur le bouton **Upload**, sélectionnez l'image à retoucher sur votre disque dur, et cliquez sur **Ouvrir**. Patientez le temps du téléchargement du fichier vers le site. Utilisez les outils proposés à gauche de la fenêtre, et les menus qui figurent en haut, pour retoucher Le travail achevé, cliquez sur **Save**, sous l'image, pour récupérer le fichier retouché sur votre PC.

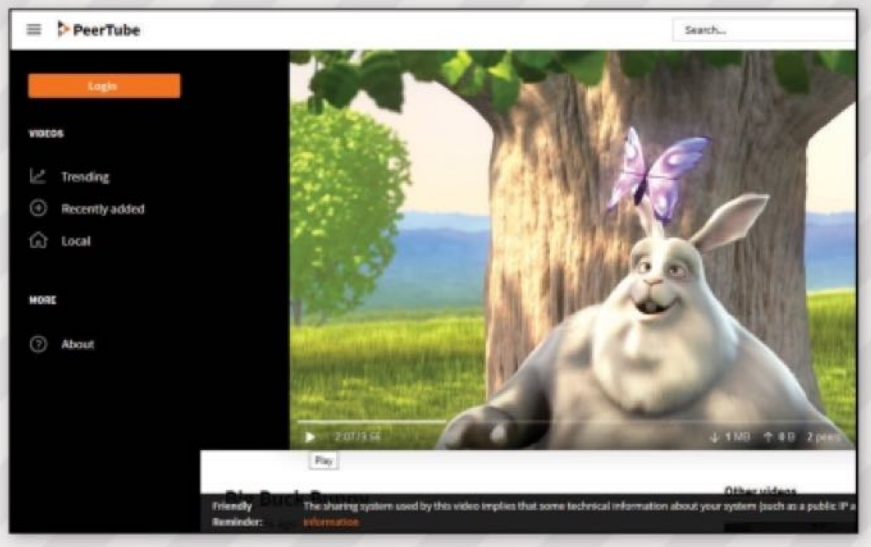
Lien : **www.lunapic.com**

#6 Reprenez le contrôle de vos vidéos

AVEC PEERTUBE

Devant la censure de YouTube, il existe des solutions comme PeerTube. N'importe qui peut héberger un serveur PeerTube qu'on nomme instance. Chaque instance héberge ses propres utilisateurs et leurs vidéos. Il garde aussi une vision des vidéos présentes sur les instances suivies par l'administrateur afin de pouvoir les proposer à ses utilisateurs. Chaque compte possède un identifiant global unique qui est composé d'un pseudonyme et du nom de domaine du serveur sur lequel il se trouve. Les administrateurs d'une instance PeerTube peuvent se suivre mutuellement. Quand votre instance PeerTube suit une autre instance PeerTube, vous recevez les informations d'affichage des vidéos de cette instance. De cette manière, vous pouvez afficher les vidéos présentes sur votre instance, et sur l'instance que vous avez décidé de suivre. Vous gardez donc le contrôle des vidéos affichées sur votre serveur.

Lien : **https://peertube.cpy.re**



#SAVE YOURINTERNET

La Commission des Affaires Juridiques (JURI) du Parlement européen vient d'approuver la directive sur la réforme du droit d'auteur. L'article 13 de cette directive européenne impose aux plates-formes Internet la mise en place d'un filtrage des contenus pour empêcher la mise en ligne de contrefaçons d'œuvres protégées.
Les défenseurs des libertés numériques appellent à se battre contre son adoption définitive...

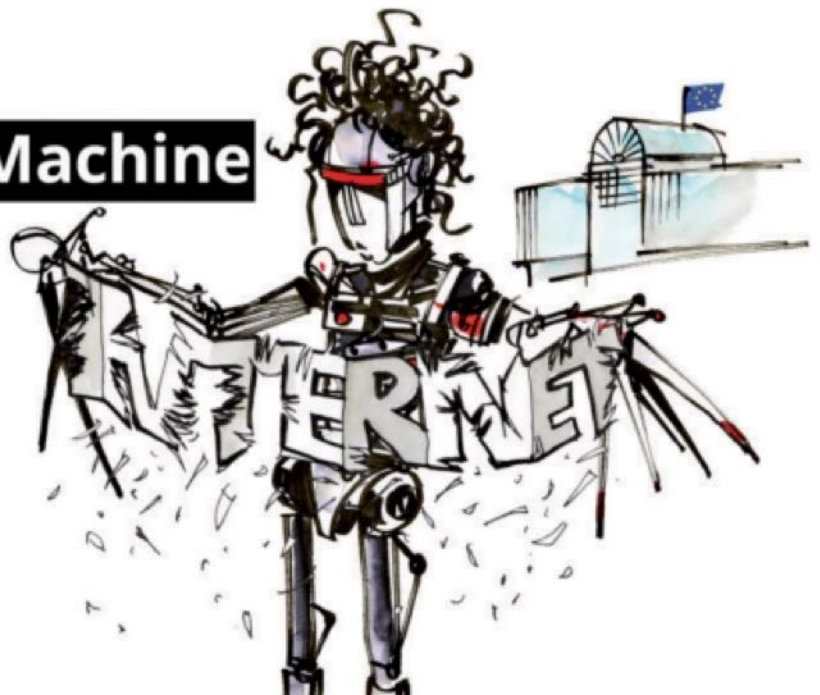
Merci à Thibaut Le Corre du Parti Pirate pour cet article ! www.partipirate.fr

Depuis quelques mois des associations et des personnalités de l'Internet font entendre leurs voix, notamment par le biais de l'Electronic Frontier Fondation dans une lettre ouverte cosignée par Tim Berners-Lee, l'inventeur du WWW afin d'éviter que ce fameux Article 13 ne « *transforme Internet en un outil de surveillance automatisé et de contrôle de ses utilisateurs* ». Julia Reda, députée européenne du Parti Pirate et fer-de-lance des opposants au texte a déclaré que « *ces mesures vont casser Internet* ».
Mais de quoi parle-t-on au juste ? Il s'agit d'imposer que tout contenu soit filtré automatiquement par les plates-formes numériques (Youtube, Facebook, Twitter, Flickr, Reddit, etc.) avant de pouvoir être partagé sur Internet. En bref que tous les contenus (vidéos, photographies, textes ou chansons) soient surveillés afin de garantir que les droits d'auteur soient respectés.

AU SECOURS CHUCK, ILS SONT DEVENUS FOUS !

Concrètement si vous partagez un élément qui ressemble à un contenu protégé par le droit d'auteur, il sera bloqué directement par la plate-forme, charge à l'internaute de faire un recours pour avoir le droit de partager son contenu.
Il s'agit là d'une inversion de la charge de la preuve, c'est aux ayants droit de saisir la justice pour faire valoir leurs droits, pas aux internautes de prouver leur bonne foi . En conséquence c'est tout ce qui fait la richesse de la culture geek et Internet qui est menacé, et chacun d'entre nous est concerné : qui n'a jamais partagé des Chuck Norris Facts ? Des parodies de Star Wars ou des couvertures de Martine via Facebook ? Des GIFs

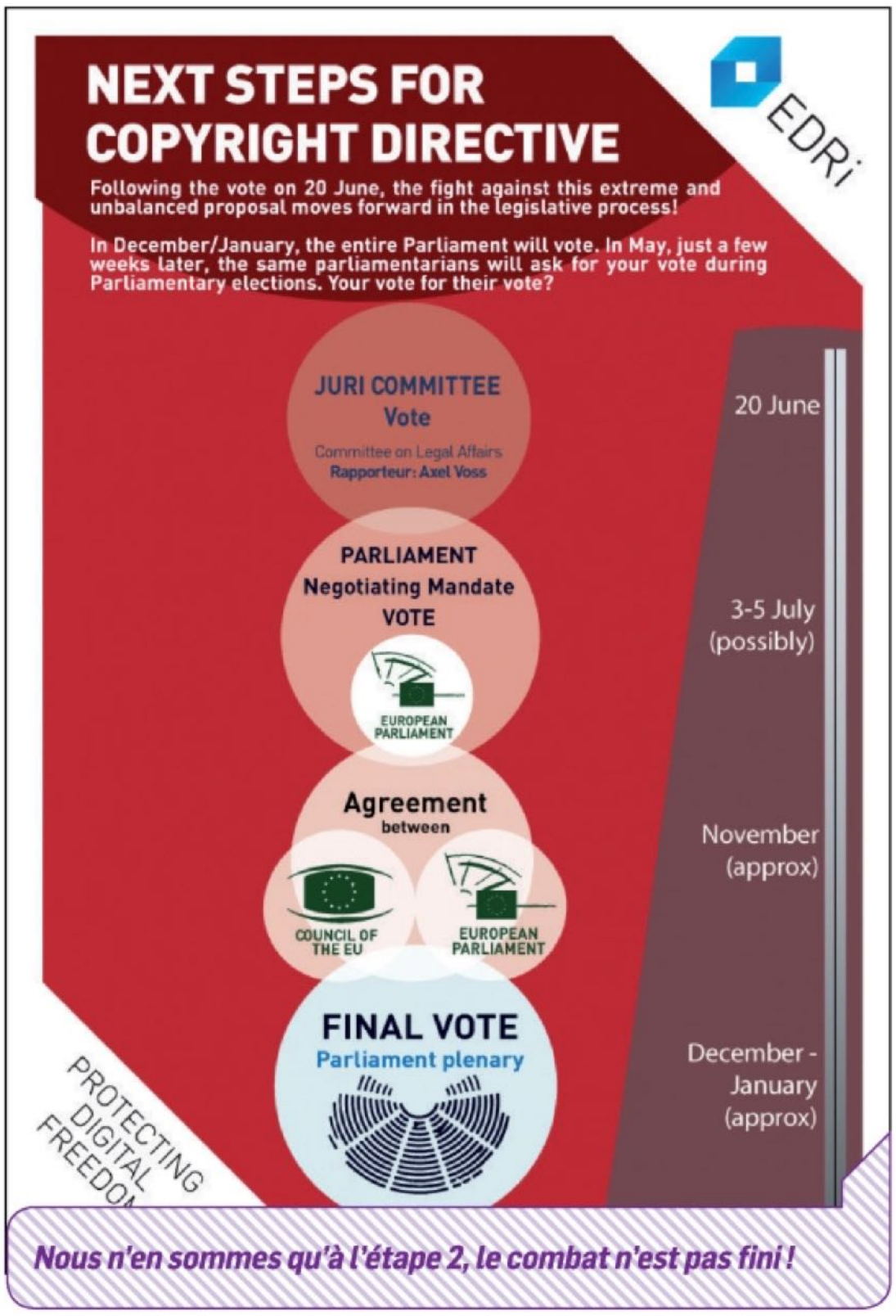
Stop the
#CensorshipMachine
Delete
Article 13



en commentaires sur Reddit ? Qui n'a jamais suivi un livestream de jeu en ligne ou fait suivre un remix via un stockage en ligne ? Au-delà de l'anecdote, c'est votre liberté d'expression qui est menacée par la mise en place d'algorithmes de filtrage par des entreprises privées !

SAUVEZ LES MÈMES PAR VOUS-MÊME !

En préparation depuis deux ans, la directive européenne du droit d'auteur est entrée dans la dernière phase avant son adoption définitive par le Parlement européen et le Conseil de l'Union européenne. Alors que les propositions de compromis du Rapport Reda (https://juliareda.eu/le-rapport-reda-explique) ont été rejetées, la directive sur la réforme du droit d'auteur est basée sur une vision répressive de ces questions au lieu de réfléchir à une évolution en profondeur des droits d'auteur rendue nécessaire par le développement du numérique dans nos vies quotidiennes. Si cette directive est adoptée, elle sera ensuite transcrite dans le droit français et il sera encore plus difficile d'agir. Vous avez la possibilité d'agir en faisant pression sur les députés européens, ce sont VOS représentants au Parlement européen, à ce titre le lobbying citoyen peut être couronné de succès comme lors du rejet de l'accord commercial anti-contrefaçon ACTA en 2012 ou pour défendre la Neutralité du Net en 2015. Vous pouvez agir en temps que citoyen européen, alors : Go, Go, Go ! Une première bataille a été gagnée lors de la réunion en séance plénière du 4 juillet 2018 le Parlement européen n'a pas donné mandat à l'eurodéputé Axel Voss, rapporteur de la commission JURI, pour négocier le texte avec la Commission européenne. Cette décision va permettre un véritable débat au Parlement européen au mois de septembre 2018 ! Prise à une large majorité (276 voix pour, 318 contre et 31 abstentions) cette décision ne reflète pas hélas les positions des eurodéputés français qui ont eux voté largement pour ce mandat de négociation empêchant un débat démocratique plus large. Les votes de nos représentants français donnent 61 pour, 8 contre et 5 non-votants... Les seuls eurodéputés français s'étant prononcés contre : Bay (ENF), D'Ornano (EFDD), Durand, Jadot (Verts/ALE), Joly (Verts/ALE), Montel (EFDD), Philippot (EFDD), Vergiat (GUE/NGL) et non votants: Jamet (ENF), JM Le Pen (NI), Manscour (S&D), Muselier, Ponga (PPE). Tous les autres ont voté pour, autant dire que nous avons en France un lobby de l'industrie culturelle très efficace auprès de nos élus. Le Parti Pirate soutient la création artistique et culturelle, mais cela ne doit pas se faire au détriment des libertés fondamentales.



POUR SAUVER INTERNET DÉCENTRALISONS-LE !

L'Europe a un fonctionnement complexe et démocratiquement illisible pour le citoyen, mais chacun d'entre nous peut exercer son droit d'interpellation auprès de ses eurodéputés pour attirer leur attention sur l'importance que leur vote peut avoir sur ce sujet en particulier. Dans l'optique de mobilisation citoyenne, l'initiative https://saveyourinternet.eu et le hashtag #SaveYourInternet ont été mis en place. Il est possible à partir de ce site d'interpeller directement vos élus européens via mails, tweets ou appels téléphoniques gratuits. Hélas, nombre de nos

élus européens ne comprennent pas la culture Internet, la soif de connaissances des internautes et le danger que peut représenter l'automatisation du filtrage des contenus en ligne. Cette plate-forme d'interpellation citoyenne vous donne les outils pour influer sur le cours des votes au niveau européen, il s'agit d'une initiative à l'échelle d'un continent, l'ensemble des citoyens doit se mobiliser : ensemble nous pouvons sauver Internet ! Cependant ne nous leurrons pas, le solutionnisme technologique prôné par l'Article 13 de cette directive européenne et plus généralement la surveillance de masse est rendu possible par la centralisation du Web et l'hégémonie de quelques plates-formes numériques. C'est à ce niveau-là que se situe la racine du problème, la décentralisation des services permettant de conserver un Internet ouvert est et reste une nécessité. Hélas le manque de culture numérique de nos représentants les rend vulnérables au lobbying des ayants droit sans prise en compte des enjeux d'un Internet ouvert. La mise en place d'une telle automatisation va mécaniquement renforcer les grandes plates-formes numériques en élevant des barrières pour les nouveaux entrants en matière d'investissement : des algorithmes de détection de fraudes existent comme le "Content ID" de Google, mais ont coûté plus de 100 millions de dollars d'investissement et n'ont à l'heure actuelle pas d'équivalent libre. Luttons contre cet Article 13, mais ne perdons pas de vue que l'objectif que nous devons poursuivre collectivement est plus large et comme le dit avec justesse Framasoft : « *La voie est longue, mais la voie est libre !* ».

La France est le pays qui a le plus voté pour le Oui. Qu'est-ce qui cloche chez nos élus?

INTERVIEW
de Julia Reda, députée européenne et membre du Parti Pirate ALLEMAND

Julia Reda est une femme politique allemande. Élue en 2014, elle est l'unique représentante du Parti Pirate au Parlement européen. Chargée par celui-ci de préparer un rapport sur la mise en œuvre de la directive 2001/29/CE7 concernant l'harmonisation du droit d'auteur en Europe, elle est maintenant le porte-étendard des opposants à l'article 13.

LE 5 JUILLET DERNIER MARQUE UN TOURNANT DANS LE COMBAT MENÉ PAR LES OPPOSANTS À LA DIRECTIVE SUR LE DROIT D'AUTEUR. MAIS CE N'EST PAS LA FIN DE L'HISTOIRE N'EST-CE PAS ?

Pour le moment, le Parlement européen a seulement décidé que le texte adopté par la commission des affaires juridiques n'était pas suffisamment équilibré pour entamer immédiatement des négociations avec le Conseil et devrait faire l'objet d'un débat plénier complet, avec la possibilité d'apporter des changements. Ce débat aura lieu lors de la session plénière de septembre. Compte tenu de la très faible majorité avec laquelle le droit voisin des éditeurs de presse a été adopté en commission, ainsi que des

protestations générales contre les filtres de téléchargement, les articles 11 et 13 devront certainement subir quelques changements. Il y a aussi beaucoup de déception de la part de la communauté de la recherche et de l'innovation sur l'approche très peu ambitieuse du comité des affaires juridiques sur le text mining et le data mining. J'espère que, avant le vote de septembre, nous serons en mesure de négocier de larges compromis sur ces articles qui seront approuvés par les deux parties au débat. Si ce n'est pas possible, on peut s'attendre à un autre vote très serré en septembre. Il est donc très important de maintenir la pression publique et de faire comprendre aux députés que leurs électeurs suivent de près ce vote. C'est pourquoi j'ai appelé à une journée d'action à l'échelle de l'UE pour une meilleure réforme du droit d'auteur le 26 août.

LA PROCHAINE ÉCHÉANCE CONCERNE LA TAXATION DES LIENS CENSÉE «SAUVER LE JOURNALISME». LES POLITICIENS ET CERTAINS MÉDIAS EXPLIQUENT QUE C'EST UNE BONNE CHOSE. QU'EST-CE QUI CLOCHE AVEC CET ARTICLE 11 ?

Depuis la convention de Berne, il était clair que la loi sur le droit d'auteur ne devrait jamais s'appliquer aux actualités. Les créations originales des journalistes sont protégées par le droit d'auteur, mais un simple titre tel que "Angela Merkel rencontre Theresa May" n'est pas protégé par un quelconque copyright, car cela entraverait la libre circulation de l'information et le débat démocratique. Un droit voisin pour les éditeurs de presse s'appliquerait à ces phrases non originales. Même un lien vers un article de presse qui utiliserait le titre en question serait soumis à une rétribution. Cela limite non seulement l'accès du public à des actualités de qualité, mais serait aussi préjudiciable pour les petits éditeurs qui dépendent des visites générées par des liens provenant des médias sociaux et d'autres sites Web.

DEPUIS LA CRÉATION DE NOTRE MAGAZINE NOUS NOUS RENDONS COMPTE QUE LA MÉCONNAISSANCE DE NOS POLITICIENS CONCERNANT LES SUJETS LIÉS À L'INFORMATIQUE ET À INTERNET RENDENT DIFFICILES CERTAINS DÉBATS. VOUS DEVEZ LES CONVAINCRE UN PAR UN ?

Je ne pense pas que tous les politiciens qui ont voté pour la directive sur le droit d'auteur soient ignorants. Je pense plutôt que beaucoup ont eu des expériences principalement négatives avec Internet et considèrent donc que tout moyen de renforcer la protection des droits des titulaires de droits est justifié, car ils ne considèrent pas nécessairement les dommages collatéraux à l'écosystème Internet comme un problème sérieux. C'est pourquoi il est très important pour les électeurs de contacter ces députés et de leur dire l'autre côté de l'histoire - comment Internet les a aidés à s'informer, à s'organiser et à devenir autonomes. Bien sûr, il existe aujourd'hui de nombreux problèmes liés au droit d'auteur sur Internet, mais pour les résoudre, nous devons analyser ces problèmes avec attention et ne pas viser des solutions simplistes.

RENFORCER LA PROTECTION DU DROIT D'AUTEUR ET L'UNIFIER AU NIVEAU EUROPÉEN EST UNE INTENTION LOUABLE À LA BASE. LA TÂCHE N'EST-ELLE PAS HERCULÉENNE AVEC TOUS CES GROUPES DE PRESSION ET CES INTÉRÊTS DIVERGENTS ?

En effet, il est incroyablement difficile de faire des progrès significatifs vers une harmonisation du droit d'auteur. Mais je crois que chaque fois qu'une proposition draconienne est rejetée par le Parlement en raison de la pression publique, cela crée une certaine marge pour des idées plus progressistes. Après le rejet du traité ACTA en 2012, quelques changements positifs ont été apportés au régime du droit d'auteur, comme la possibilité de réutiliser des œuvres orphelines (bien que cela pose encore de nombreux problèmes dans la pratique) et le renforcement de la transparence les organisations de gestion. C'est un combat difficile, mais je crois que si la résistance à ces lois strictes sur le droit d'auteur continue de se faire sentir, des changements significatifs dans l'autre direction seront possibles.

LE PARTI PIRATE A BESOIN DE VOUS !

Fondé en 2006, Le Parti pirate est un parti politique créé sur le modèle de son homologue suédois. Sa devise est « liberté, démocratie, partage ». Son programme se développe sur la base de la protection des droits et libertés fondamentales, aussi bien dans le domaine numérique qu'en dehors : légalisation du partage hors marché, la lutte contre le fichage abusif, l'indépendance de la justice, la transparence de la vie politique et l'ouverture des données publiques.

Si vous voulez adhérer : **https://adhesion.partipirate.org**

Si vous souhaitez faire un don : **https://don.partipirate.org**

LE FORUM
DE LA COMMUNAUTÉ
Android MT

forum.android-mt.com

Tutoriels · Conseils & astuces · **Tests** · Avis ·
Dépannage · **Hacking** · Découverte d'applications...

LE MAILING-LIST OFFICIELLE de

Pirate Informatique et des *Dossiers du Pirate*

INSCRIVEZ-VOUS GRATUITEMENT !

De nombreux lecteurs nous demandent chaque jour s'il est possible de s'abonner. La réponse est non et ce n'est malheureusement pas de notre faute. En effet, nos magazines respectent la loi, traitent d'informations liées au monde du hacking au sens premier, celui qui est synonyme d'innovation, de créativité et de liberté. Depuis les débuts de l'ère informatique, les hackers sont en première ligne pour faire avancer notre réflexion, nos standards et nos usages quotidiens.

Mais cela n'a pas empêché notre administration de référence, la «Commission paritaire des publications et agences de presse» (CPPAP) de refuser nos demandes d'inscription sur ses registres. En bref, l'administration considère que ce que nous écrivons n'intéresse personne et ne traite pas de sujets méritant débat et pédagogie auprès du grand public. Entre autres conséquences pour la vie de nos magazines : pas d'abonnements possibles, car nous ne pouvons pas bénéficier des tarifs presse de la Poste. Sans ce tarif spécial, nous serions obligés de faire payer les abonnés plus cher ! Le monde à l'envers...

La seule solution que nous avons trouvée est de proposer à nos lecteurs de s'abonner à une mailing-list pour les prévenir de la sortie de nos publications. Il s'agit juste d'un e-mail envoyé à tous ceux intéressés par nos magazines et qui ne veulent le rater sous aucun prétexte.

Pour en profiter, il suffit de s'abonner directement sur ce site

http://eepurl.com/FlOOD

(le L de «FlOOD» est en minuscule)

ou de scanner ce QR Code avec votre smartphone...

NOUVEAU !

La rédaction se dote d'un compte Twitter !

twitter.com/ben_IDPresse

Vous trouverez des news inédites, des liens exclusifs vers des articles au format PDF et nous vous tiendrons aussi au courant de la sortie des publications. Rejoignez-nous !

TROIS BONNES RAISONS DE S'INSCRIRE :

1. Soyez averti de la sortie de *Pirate Informatique* et des *Dossiers du Pirate* en kiosques. Ne ratez plus un numéro !
2. Vous ne recevrez qu'un seul e-mail par mois pour vous prévenir des dates de parutions et de l'avancement du magazine.
3. Votre adresse e-mail reste confidentielle et vous pouvez vous désabonner très facilement. Notre crédibilité est en jeu.

Votre marchand de journaux n'a pas *Pirate Informatique* ou *Les Dossiers du Pirate* ?

Si votre marchand de journaux n'a pas le magazine en kiosque, il suffit de lui demander (gentiment) de vous commander l'exemplaire auprès de son dépositaire. Pour cela, munissez-vous du numéro de codification L12730 pour *Pirate Informatique* ou L14376 pour *Les Dossiers du Pirate*.

Conformément à la loi «informatique et libertés» du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent.

X-MATÉRIELS

> Bare Conductive Electric Paint

Réservée à ceux ayant soutenu le projet sur Kick Starter, la peinture conductive de Bare Conductive est disponible à tout un chacun sur le marché. Elle est disponible en tube de 10 ml ou en pot de 50 ml. Il s'agit en fait d'une peinture qui conduit l'électricité ! Il est donc possible de peindre des fils ou des capteurs directement sur presque tous les matériaux, y compris le papier, le bois, le plastique, les textiles, le carton et le verre. Le tube de 10ml est parfait pour les petits projets ou pour la peinture, la soudure ou la réparation de petites cassures. Non toxique, sans solvant et soluble dans l'eau, les tubes de 10 ml de peinture électrique sont idéals pour le prototypage et sans danger pour les makers. La peinture sèche en un quart d'heure et est facilement effaçable au savon. Maintenue au sec, la peinture peut durer des années.

Prix : **12 €** **https://tinyurl.com/yd3kcpoz - www.kubii.fr**

> GrayKey de Grayshift

Vous avez déjà entendu parler de la difficulté que les hackers ont à craquer la protection par mot de passe des iPhones. Cela ne va pas aller en s'améliorant puisqu'une nouvelle fonctionnalité va bientôt faire son apparition dans la prochaine mise à jour d'iOS (mais déjà présente dans les versions bêta). Il s'agit en fait d'ajouter une restriction au niveau de la connexion USB : il faudra s'authentifier toutes les heures. Dans le cas contraire, l'accès aux données sera coupé. Il s'agit pour Apple de protéger ses appareils des tentatives de brute force (de pirate ou du FBI). Il est peu probable que l'opération dure moins d'une heure (comptez plusieurs jours pour un mot de passe de 9 caractères). La société Grayshift a trouvé la parade avec son boîtier GrayKey. Non content d'avoir été les premiers à trouver une faille dans le système de protection d'Apple (et de l'avoir gardé pour soi), leur petite boîte ne serait pas concernée par cette nouvelle restriction USB, pas plus que la limitation à trois tentatives de code. Vous aimeriez tester la GrayKey ? Il faudra montrer patte blanche et débourser... 15 000 $.

Prix : **15 000 $**

https://graykey.grayshift.com

> Nuxii :

LE BOÎTIER ULTIME POUR VOTRE RASPBERRY PI

Il existe quantité de boîtiers permettant d'abriter un Raspberry Pi, mais le Nuxii fait figure de Roll's Royce dans ce domaine. Livré en kit, il comprend différents éléments modulables qui le rendent indispensable pour les utilisateurs désirant se confectionner une mini-console, un streamer audio, un media center, un serveur ou un mini-PC. La version qui nous a été prêtée par le fabricant coûte 25 €, mais sur le site vous pouvez ajouter les options que vous voulez: module infrarouge + télécommande, écran LCD latéral, LED RGB, bouton poussoir pour l'allumage/l'extinction, des capots de matières et couleurs différentes pour refermer le contenu. Au final, notre version « media center » nous aura coûté un peu plus de 40 €. Certes c'est cher, mais c'est aussi le prix de la qualité et de la sécurité, car à l'inverse de beaucoup de ses concurrents, le bouton poussoir est relié au port GPIO pour éteindre «proprement» un OS : il ne s'agit pas d'un simple mode OFF qui revient à couper l'alimentation comme un sauvage. Grâce à cela, vous économiserez la durée de vie de votre carte SD. Notez que dans le Nuxii, il y a suffisamment de place pour un HAT et qu'il y a des fentes prédécoupées pour ajouter un écran LCD (par exemple). Vous trouverez des tutos détaillés sur le site du constructeur : https://tinyurl.com/yaglokpv.

Prix : Entre **25** et **50 €** **https://nuxii.fr**

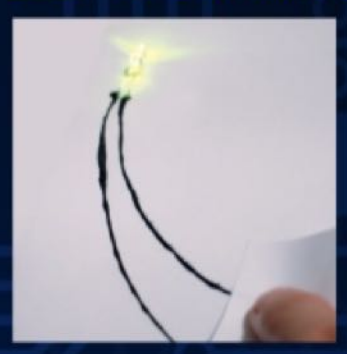
NOTRE TEST EXCLUSIF

Electric Paint
Dessinez des circuits imprimés !

Nous avons attendu longtemps avant de pouvoir faire joujou avec cette peinture électrique. Mais que peut-on faire avec cette peinture magique ?

Lien : **www.bareconductive.com**

#1 DESSINER DES CIRCUITS ÉLECTRONIQUES



Les 10 ml de peinture contenus dans le tube suffisent pour faire jusqu'à 5 m de piste pour circuit imprimé sur toutes les surfaces. Il suffit de presser le tube doucement pour appliquer une fine couche de peinture. Il faudra ensuite laisser sécher pendant 15 minutes avant de l'utiliser. Ce que vous créez n'a pas besoin de ressembler à un schéma de circuit traditionnel. Avec Electric Paint, vous pouvez créer des circuits fonctionnels et inventifs.

#2 SOUDURE À FROID

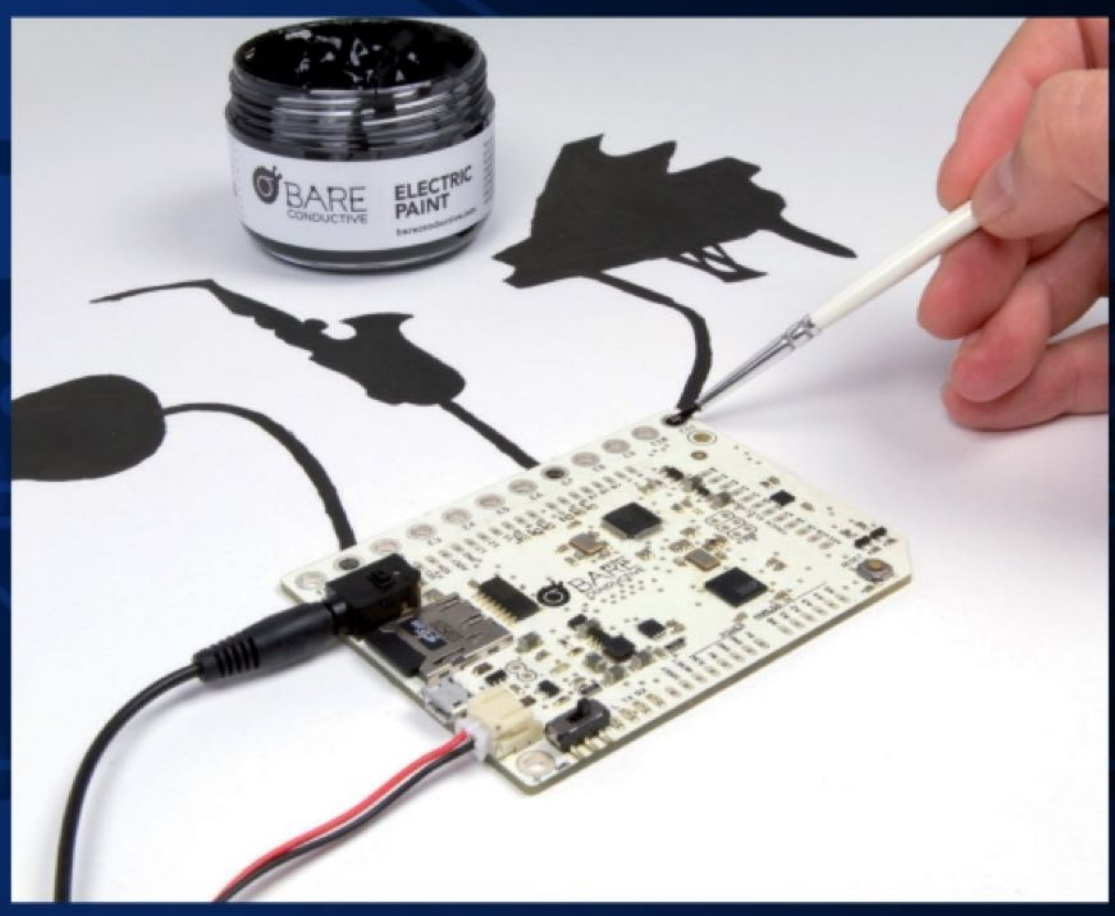
Cette peinture est aussi parfaite pour faire des points de soudure à froid grâce à sa viscosité et un caractère adhésif. Bien sûr l'ensemble ne sera pas aussi solide qu'une vraie soudure, mais elle aura le mérite d'être sans danger pour les enfants et facile à mettre en place. Placez une LED ou une résistance sur un circuit imprimé et tentez l'expérience ! Vous pouvez aussi faire un circuit électronique sur du carton ou du plastique et « souder » sur cette matière...

#3 RÉPARATION DE CIRCUIT IMPRIMÉ

Comme pour la soudure, les propriétés conductrice et adhésive de cette peinture peuvent servir à réparer des circuits imprimés. Un trou dans une piste en cuivre ? Une dérivation à faire sur un PCB défectueux, tordu ou cassé ? Il suffit de peindre vos modifications et de laisser sécher !

#4 ET BIEN PLUS ENCORE...

Pour améliorer l'expérience, la société Bare Conductive commercialise une carte appelée Touch Board. Compatible avec le langage Arduino, cette dernière permet de «jouer» avec la peinture et ses connecteurs. Dessinez des circuits et reliez-les à la carte pour programmer un ensemble. Le Touch Board starter kit (environ 130 €) comprend la carte, 60 ml de peinture, et divers accessoires pour faire des expériences : capteurs, carte micro SD, mini haut-parleur, des pochoirs, pinces crocodile, ruban de cuivre et divers câbles.



SUR NOTRE CD :

Les meilleurs logiciels et services de pros

OFFERTS

HACKING

ANONYMAT **PROTECTION**

Le GUIDE PRATIQUE DU HACKER

SOLUTIONS & ASTUCES 100% GRATUITES

IDPRESSE

L 12730 - 38 - F: 4,90 € - RD

France METRO : 4,90 € - BEL/LUX : 6 € - DOM : 6,10 € - PORT.CONT. : 6 € - CAN : 7,99 $ cad – POL/S : 750 CFP – NCAL/A : 950 CFP - MAR : 50 mad - TUN : 9,8 tnd